



SUGHRUE MION ZINN MACPEAK & SEAS, PLLC

J. Frank Osha
T 1-(202)-663-7915
fosha@sughrue.com

May 23, 2001

BOX PATENT APPLICATION
Commissioner for Patents
Washington, D.C. 20231

Re: Application of Tatsuhiro IBUKI
USER AUTHENTICATION DEVICE AND ELECTRIC COMMERCE SYSTEM
USING THE DEVICE
Assignee: NEC CORPORATION
Our Ref. Q64565

Dear Sir:

Attached hereto is the application identified above including 65 sheets of the specification, including the claims and abstract, 16 sheets of formal drawings, executed Assignment and PTO 1595 form, and executed Declaration and Power of Attorney. Also enclosed is the Information Disclosure Statement with form PTO-1449 and reference.

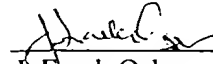
The Government filing fee is calculated as follows:

Total claims	28 - 20	=	8	x	\$18.00	=	\$144.00
Independent claims	4 - 3	=	1	x	\$80.00	=	\$80.00
Base Fee							\$710.00
TOTAL FILING FEE							\$934.00
Recordation of Assignment							\$40.00
TOTAL FEE							\$974.00

Checks for the statutory filing fee of \$934.00 and Assignment recordation fee of \$40.00 are attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 and any petitions for extension of time under 37 C.F.R. § 1.136 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

Priority is claimed from May 25, 2000 based on Japanese Application No. 2000-155140. The priority document is enclosed herewith.

Respectfully submitted,
SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
Attorneys for Applicant

By: 
J. Frank Osha
Registration No. 24,625

2100 Pennsylvania Avenue, NW
Washington, DC 20037-3213

T 202.293.7060
F 202.293.7860

1010 El Camino Real
Menlo Park, CA 94025-4345

T 650.325.5800
F 650.325.6606

Toei Nishi Shimbashi Bldg. 4F
13-5 Nishi Shimbashi 1-Chome
Minato-Ku, Tokyo 105-0003
Japan

T 03.3503.3760
F 03.3503.3756

www.sughrue.com

#2



日本国
PATENT (OFFICE)
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事
項と同一であることを証明する
This is to certify that the annexed is a true
copy of the original with this Office.

出願年月日
Date of Application:

2000年

出願番号
Application Number:

特願2000-.....

願人
Applicant(s):

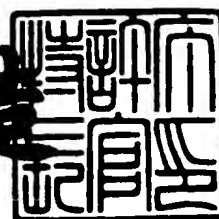
群馬日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 2月23日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3010774

【書類名】 特許願

【整理番号】 03202542

【提出日】 平成12年 5月25日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F

【発明の名称】 ユーザ認証装置及びこれを用いた商取引システム

【請求項の数】 12

【発明者】

 【住所又は居所】 群馬県太田市西矢島町 3 2 番地 群馬日本電気株式会社
内

 【氏名】 伊吹 竜大

【特許出願人】

 【識別番号】 000165033

 【氏名又は名称】 群馬日本電気株式会社

【代理人】

 【識別番号】 100079164

 【弁理士】

 【氏名又は名称】 高橋 勇

 【電話番号】 03-3862-6520

【手数料の表示】

 【予納台帳番号】 013505

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9003383

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ユーザ認証装置及びこれを用いた商取引システム

【特許請求の範囲】

【請求項 1】 通信ネットワークを介して接続されたユーザ側情報処理部及び認証側情報処理部を備えたユーザ認証装置であって、

前記ユーザ側情報処理部は、

第一の認証用番号を前記認証側情報処理部へ送信する機能と、

前記認証側情報処理部からアクセス許可通知を受信すると、所定の変換則を用いて当該第一の認証用番号を第二の認証用番号に変換し、この第二の認証用番号を新たな第一の認証用番号とする機能とを有し、

前記認証側情報処理部は、

前記ユーザ側情報処理部から前記第一の認証用番号を受信すると、データベースを用いて照合処理を実行する機能と、

この照合処理によって正規ユーザであると認証すると、アクセス許可通知を前記ユーザ側情報処理部へ送信する機能と、

前記アクセス許可通知を送信すると、前記変換則と同じものを用いて当該第一の認証用番号を第二の認証用番号に変換し、この第二の認証用番号を新たな第一の認証用番号として前記データベースに記録する機能とを有する、

ことを特徴とするユーザ認証装置。

【請求項 2】 前記ユーザ側情報処理部は、携帯型記録媒体を備えるとともに、

この携帯型記録媒体から第一の認証用番号及び所定の変換則を読み取り当該第一の認証用番号を前記認証側情報処理部へ送信する機能と、

前記アクセス許可通知を受信すると、前記変換則を用いて当該第一の認証用番号を第二の認証用番号に変換し、この第二の認証用番号を新たな第一の認証用番号として前記携帯型記録媒体に記録する機能とを有する、

請求項 1 記載のユーザ認証装置。

【請求項 3】 前記ユーザ側情報処理部は、携帯型記録媒体を備えるとともに、この携帯型記録媒体から第一の認証用番号を読み取り当該第一の認証用番号

を前記認証側情報処理部へ送信する機能を有し、

前記携帯型記録媒体は、前記アクセス許可通知が受信されると、所定の変換則を用いて当該第一の認証用番号を第二の認証用番号に変換し、この第二の認証用番号を新たな第一の認証用番号として当該携帯型記録媒体に記録する機能を有する、

請求項 1 記載のユーザ認証装置。

【請求項 4】 前記ユーザ側情報処理部は、携帯型記録媒体を備えとともに、

第一の認証用番号を入力して当該第一の認証用番号を前記認証側情報処理部へ送信する機能と、

前記携帯型記録媒体から所定の変換則を読み取るとともに、前記アクセス許可通知を受信すると、前記変換則を用いて当該第一の認証用番号を第二の認証用番号に変換し、この第二の認証用番号を新たな第一の認証用番号として出力する機能とを有する、

請求項 1 記載のユーザ認証装置。

【請求項 5】 通信ネットワークを介して接続されたユーザ側情報処理部、仲介側情報処理部及び認証側情報処理部を備えたユーザ認証装置であって、

前記ユーザ側情報処理部は、

第一の認証用番号を前記仲介側情報処理部へ送信する機能と、

前記仲介側情報処理部から第二の認証用番号を受信すると、所定の変換則を用いて当該第二の認証用番号を第三の認証用番号に変換し、この第三の認証用番号を新たな第一の認証用番号とする機能とを有し、

前記仲介側情報処理部は、

前記ユーザ側情報処理部から送信された前記第一の認証用番号を前記認証側情報処理部へ送信する機能と、

前記認証側情報処理部から前記第二の認証用番号を受信し、この第二の認証用番号を前記ユーザ側情報処理部へ送信する機能とを有し、

前記認証側情報処理部は、

前記仲介側情報処理部から前記第一の認証用番号を受信すると、データベース

を用いて照合処理を実行し、この照合処理によって正規ユーザであると認証すると、前記第一の認証用番号とは異なる前記第二の認証用番号を前記仲介側情報処理部へ送信する機能と、

前記変換則と同じものを用いて前記第二の認証用番号を第三の認証用番号に変換し、この第三の認証用番号を新たな第一の認証用番号として前記データベースに記録する機能とを有する、

ことを特徴とするユーザ認証装置。

【請求項 6】 前記ユーザ側情報処理部は、携帯型記録媒体を備えるとともに、

この携帯型記録媒体から第一の認証用番号及び所定の変換則を読み取り当該第一の認証用番号を前記仲介側情報処理部へ送信する機能と、

前記第二の認証用番号を受信すると、前記変換則を用いて当該第二の認証用番号を第三の認証用番号に変換し、この第二の認証用番号を新たな第一の認証用番号として前記携帯型記録媒体に記録する機能とを有する、

請求項 5 記載のユーザ認証装置。

【請求項 7】 前記ユーザ側情報処理部は、携帯型記録媒体を備えるとともに、この携帯型記録媒体から第一の認証用番号を読み取り当該第一の認証用番号を前記仲介側情報処理部へ送信する機能を有し、

前記携帯型記録媒体は、前記第二の認証用番号を受信されると、所定の変換則を用いて当該第二の認証用番号を第三の認証用番号に変換し、この第三の認証用番号を新たな第一の認証用番号として当該携帯型記録媒体に記録する機能を有する、

請求項 5 記載のユーザ認証装置。

【請求項 8】 前記ユーザ側情報処理部は、携帯型記録媒体を備えるとともに、

第一の認証用番号を入力して当該第一の認証用番号を前記仲介側情報処理部へ送信する機能と、

前記携帯型記録媒体から所定の変換則を読み取るとともに、前記第二の認証用番号を受信すると、前記変換則を用いて当該第二の認証用番号を第三の認証用番

号に変換し、この第三の認証用番号を新たな第一の認証用番号として出力する機能とを有する、

請求項 5 記載のユーザ認証装置。

【請求項 9】 請求項 2 又は 3 記載のユーザ認証装置を用いた商取引システムであって、

前記ユーザ側情報処理部は前記第一の認証用番号とともに決済要求を前記認証側情報処理部へ送信し、

前記認証側情報処理部は前記照合処理とともに決済処理を実行し、

前記通信ネットワークがインターネット、

前記ユーザ側情報処理部が店頭端末、

前記認証側情報処理部がクレジット会社端末、

前記携帯型記録媒体がクレジットカード、

前記認証用番号がクレジット番号である、

ことを特徴とする商取引システム。

【請求項 10】 請求項 4 記載のユーザ認証装置を用いた商取引システムであって、

前記ユーザ側情報処理部は前記第一の認証用番号とともに決済要求を前記認証側情報処理部へ送信し、

前記認証側情報処理部は前記照合処理とともに決済処理を実行し、

前記通信ネットワークがインターネット、

前記ユーザ側情報処理部が店頭端末、

前記認証側情報処理部が銀行端末、

前記携帯型記録媒体がキャッシュカード、

前記認証用番号が暗証番号である、

ことを特徴とする商取引システム。

【請求項 11】 請求項 6 又は 7 記載のユーザ認証装置を用いた商取引システムであって、

前記仲介側情報処理部は前記第一の認証用番号とともに決済要求を前記認証側情報処理部へ送信し、

前記認証側情報処理部は前記照合処理とともに決済処理を実行し、
 前記通信ネットワークがインターネット、
 前記ユーザ側情報処理部がユーザ端末、
 前記仲介側情報処理部が販売センター端末、
 前記認証側情報処理部がクレジット会社端末、
 前記携帯型記録媒体がクレジットカード、
 前記認証用番号がクレジット番号である、
 ことを特徴とする商取引システム。

【請求項 1 2】 請求項 8 記載のユーザ認証装置を用いた商取引システムであって、

前記仲介側情報処理部は前記第一の認証用番号とともに決済要求を前記認証側情報処理部へ送信し、

前記認証側情報処理部は前記照合処理とともに決済処理を実行し、
 前記通信ネットワークがインターネット、
 前記ユーザ側情報処理部がユーザ端末、
 前記仲介側情報処理部が販売センター端末、
 前記認証側情報処理部が銀行端末、
 前記携帯型記録媒体がキャッシュカード、
 前記認証用番号が暗証番号である、
 ことを特徴とする商取引システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、通信ネットワークを介して送受信される認証用番号を使ってユーザを認証するためのユーザ認証装置、及びこのユーザ認証装置を用いた商取引システムに関する。認証用番号としては、例えばクレジット番号、暗証番号、ID番号、パスワード等が挙げられる。なお、「認証」とは、システムの利用者に対して申告した本人であるかどうかの正当性を確認すること（authentication）、又はあるシステム資源に対してアクセス権限を持っているかどうかを確認して使用

権限を与えること (authorization) と定義されている (日経 B P 社刊「通信・ネットワーク用語ハンドブック 2 0 0 0 年版」)。

【 0 0 0 2 】

【従来の技術】

インターネット上での商取引における支払いの方法として、クレジットカードを利用する方法がある。クレジットカードを利用した従来の支払方法は、注文者が氏名及びクレジットカード番号をユーザ端末を用いて販売センターに送出し、販売センターがクレジット会社にアクセスして決済の処理を行うというものである。

【 0 0 0 3 】

【発明が解決しようとする課題】

しかしながら、この従来の方法には次のような問題があった。

【 0 0 0 4 】

ユーザ端末－販売センター端末間及び販売センター端末－クレジット会社端末間のデータ送受信にインターネットを用いるため、インターネットを介して情報が第三者に盗まれる可能性があった。その結果、盗まれたクレジットカード番号を第三者に悪用される危険性があった。いわゆる「なりすまし」である。

【 0 0 0 5 】

【発明の目的】

そこで、本発明の目的は、通信ネットワークを介して送受信されるクレジットカード番号等が第三者に盗まれた場合でも、悪用されることのないユーザ認証装置、及びこのユーザ認証装置を用いた商取引システムを提供することにある。

【 0 0 0 6 】

【課題を解決するための手段】

図 1 は請求項 1 記載のユーザ認証装置を示し、図 1 [1] はブロック図、図 1 [2] はシーケンス図である。以下、これらの図面に基づき説明する。

【 0 0 0 7 】

請求項 1 記載のユーザ認証装置は、通信ネットワーク 1 を介して接続されたユーザ側情報処理部 2 及び認証側情報処理部 3 を備えたものである。そして、ユーザ側情報処理部 2 は、第一の認証用番号を認証側情報処理部 3 へ送信する機能と

、認証側情報処理部 3 からアクセス許可通知を受信すると、所定の変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し、第二の認証用番号を新たな第一の認証用番号とする機能とを有する。認証側情報処理部 3 は、ユーザ側情報処理部 2 から第一の認証用番号を受信すると、データベース 5 を用いて照合処理を実行する機能と、この照合処理によって正規ユーザであると認証すると、アクセス許可通知をユーザ側情報処理部 2 へ送信する機能と、アクセス許可通知を送信すると、変換則 4 と同じものを用いて第一の認証用番号を第二の認証用番号に変換し、第二の認証用番号を新たな第一の認証用番号としてデータベース 5 に記録する機能とを有する。

【 0 0 0 8 】

まず、ユーザ側情報処理部 2 は、第一の認証用番号を認証側情報処理部 3 へ送信する（ステップ 1 0 1）。認証側情報処理部 3 は、第一の認証用番号を受信すると、データベース 5 を用いて照合処理を実行する（ステップ 1 0 2）。そして、この照合処理によって正規ユーザであると認証すると、アクセス許可通知をユーザ側情報処理部 2 へ送信する（ステップ 1 0 3）。続いて、変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し（ステップ 1 0 4）、第二の認証用番号を新たな第一の認証用番号としてデータベース 5 に記録する（ステップ 1 0 5）。一方、ユーザ側情報処理部 2 は、アクセス許可通知を受信すると、変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し、第二の認証用番号を新たな第一の認証用番号とする（ステップ 1 0 6）。なお、ステップ 1 0 2 の照合処理において正規ユーザであると認められない場合は、その後の処理が実行されない。

【 0 0 0 9 】

ここで、例えば通信ネットワーク 1 を介して、正規ユーザ以外の第三者によって認証用番号が知られてしまったとする。そして、その第三者がその認証用番号を使って認証側情報処理部 3 に対するアクセスを試みたとする。しかし、認証側情報処理部 3 では、その認証用番号が既に変換されているので、そのアクセスが許可されることはない。したがって、「なりすまし」による不当なアクセスが防止される。また、ユーザ側情報処理部 2 では、認証側情報処理部 2 と同じ変換則

によって認証用番号が変換されているので、その変換後の認証用番号を使って認証側情報処理部 2 へアクセスすることができる。

【0010】

なお、ユーザ側情報処理部 2 は、例えばマイクロコンピュータ内蔵の携帯電話機、パーソナルコンピュータ等である。認証側情報処理部 3 は、例えばサーバー用コンピュータ、パーソナルコンピュータ等である。認証用番号とは、クレジット番号、暗証番号、ID 番号、パスワード等である。ユーザとは、個人、法人、複数の人が所属するグループ等である。

【0011】

次に、請求項 1 記載のユーザ認証装置の下位概念として、ユーザ側情報処理部に携帯型記録媒体を具備させた例を、請求項 2 乃至 4 記載のユーザ認証装置として示す。

【0012】

図 2 は請求項 2 記載のユーザ認証装置を示し、図 2 [1] はブロック図、図 2 [2] はシーケンス図である。以下、この図面に基づき説明する。

【0013】

請求項 2 記載のユーザ認証装置は、請求項 1 記載のユーザ認証装置において、ユーザ側情報処理部 2 が携帯型記録媒体 6 を備えるものである。そして、ユーザ側情報処理部 2 は、携帯型記録媒体 6 から第一の認証用番号及び所定の変換則 4 を読み取り第一の認証用番号を認証側情報処理部 3 へ送信する機能と、アクセス許可通知を受信すると、変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し、第二の認証用番号を新たな第一の認証用番号として携帯型記録媒体 6 に記録する機能とを有する。

【0014】

まず、ユーザ側情報処理部 2 は、携帯型記録媒体 6 から第一の認証用番号及び所定の変換則 4 を読み取り（ステップ 110, 111）、第一の認証用番号を認証側情報処理部 3 へ送信する（ステップ 101）。認証側情報処理部 3 は、第一の認証用番号を受信すると、データベース 5 を用いて照合処理を実行する（ステップ 102）。そして、この照合処理によって正規ユーザであると認証すると、

アクセス許可通知をユーザ側情報処理部 2 へ送信する（ステップ 103）。続いて、変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し（ステップ 104）、第二の認証用番号を新たな第一の認証用番号としてデータベース 5 に記録する（ステップ 105）。一方、ユーザ側情報処理部 2 は、アクセス許可通知を受信すると、変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し（ステップ 106）、第二の認証用番号を新たな第一の認証用番号として携帯型記録媒体 6 に記録する（ステップ 112, 113）。

【0015】

請求項 2 記載のユーザ認証装置も、請求項 1 記載のユーザ認証装置と同等の作用及び効果を奏する。携帯型記録媒体 6 としては、認証用番号及び変換則の記録ができるだけの少ないメモリ容量でよいので、磁気カードが適している。この場合、ユーザ側情報処理部 2 は、カードリーダー・ライタを備えたものとなる。

【0016】

図 3 は請求項 3 記載のユーザ認証装置を示し、図 3 [1] はブロック図、図 3 [2] はシーケンス図である。以下、この図面に基づき説明する。

【0017】

請求項 3 記載のユーザ認証装置は、請求項 1 記載のユーザ認証装置において、ユーザ側情報処理部 2 が携帯型記録媒体 6 を備えるものである。そして、ユーザ側情報処理部 2 は、携帯型記録媒体 6 から第一の認証用番号を読み取り第一の認証用番号を認証側情報処理部 3 へ送信する機能を有する。携帯型記録媒体 6 は、アクセス許可通知が受信されると、所定の変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し、この第二の認証用番号を新たな第一の認証用番号として携帯型記録媒体 6 に記録する機能を有する。

【0018】

まず、ユーザ側情報処理部 2 は、携帯型記録媒体 6 から第一の認証用番号を読み取り（ステップ 120, 121）、第一の認証用番号を認証側情報処理部 3 へ送信する（ステップ 101）。認証側情報処理部 3 は、第一の認証用番号を受信すると、データベース 5 を用いて照合処理を実行する（ステップ 102）。そして、この照合処理によって正規ユーザであると認証すると、アクセス許可通知を

ユーザ側情報処理部 2 へ送信する（ステップ 1 0 3）。続いて、変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し（ステップ 1 0 4）、第二の認証用番号を新たな第一の認証用番号としてデータベース 5 に記録する（ステップ 1 0 5）。一方、ユーザ側情報処理部 2 がアクセス許可通知を受信すると（ステップ 1 2 2）、携帯型記録媒体 6 は、変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し（ステップ 1 2 3）、第二の認証用番号を新たな第一の認証用番号として携帯型記録媒体 6 に記録する（ステップ 1 2 4）。

【 0 0 1 9 】

請求項 3 記載のユーザ認証装置も、請求項 1 記載のユーザ認証装置と同等の作用及び効果を奏する。携帯型記録媒体 6 としては、認証用番号を変換する演算機能が必要になるので、IC カードが適している。この場合、ユーザ側情報処理部 2 は、IC カードコネクタを備えたものとなる。

【 0 0 2 0 】

図 4 は請求項 4 記載のユーザ認証装置を示し、図 4 [1] はブロック図、図 4 [2] はシーケンス図である。以下、この図面に基づき説明する。

【 0 0 2 1 】

請求項 4 記載のユーザ認証装置は、請求項 1 記載のユーザ認証装置において、ユーザ側情報処理部 2 が携帯型記録媒体 6 を備えるものである。そして、ユーザ側情報処理部 2 は、第一の認証用番号を入力して第一の認証用番号を認証側情報処理部 3 へ送信する機能と、携帯型記録媒体 6 から所定の変換則を読み取るとともに、アクセス許可通知を受信すると、変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し、この第二の認証用番号を新たな第一の認証用番号として出力する機能とを有する。

【 0 0 2 2 】

まず、ユーザ側情報処理部 2 は、第一の認証用番号を入力し（ステップ 1 3 0）、第一の認証用番号を認証側情報処理部 3 へ送信する（ステップ 1 0 1）。認証側情報処理部 3 は、第一の認証用番号を受信すると、データベース 5 を用いて照合処理を実行する（ステップ 1 0 2）。そして、この照合処理によって正規ユーザであると認証すると、アクセス許可通知をユーザ側情報処理部 2 へ送信する

(ステップ103)。続いて、変換則4を用いて第一の認証用番号を第二の認証用番号に変換し(ステップ104)、第二の認証用番号を新たな第一の認証用番号としてデータベース5に記録する(ステップ105)。一方、ユーザ側情報処理部2は、アクセス許可通知を受信すると携帯型記録媒体6から所定の変換則4を読み取り(ステップ131、132)、変換則4を用いて第一の認証用番号を第二の認証用番号に変換し(ステップ133)、第二の認証用番号を新たな第一の認証用番号として出力する(ステップ134)。

【0023】

請求項4記載のユーザ認証装置も、請求項1記載のユーザ認証装置と同等の作用及び効果を奏する。ステップ130における第一の認証用番号の入力は、例えばユーザによるキーボードからの入力である。ステップ134における新たな第一の認証用番号の出力は、例えばユーザだけが見ることのできるディスプレイへの表示である。携帯型記録媒体6としては、変換則の記録ができるだけの少ないメモリ容量でよいので、磁気カードが適している。認証用番号としては、携帯型記録媒体6に記録されないので、暗証番号が適している。なお、ユーザ側情報処理部2に変換則が記録されていれば、携帯型記録媒体6が不要になるが、この場合の構成は請求項1記載のユーザ認証装置に含まれる。

【0024】

図5は請求項5記載のユーザ認証装置を示し、図5[1]はブロック図、図5[2]はシーケンス図である。以下、この図面に基づき説明する。

【0025】

請求項5記載のユーザ認証装置は、通信ネットワーク1を介して接続されたユーザ側情報処理部2、仲介側情報処理部7及び認証側情報処理部3を備えたものである。ユーザ側情報処理部2は、第一の認証用番号を仲介側情報処理部7へ送信する機能と、仲介側情報処理部7から第二の認証用番号を受信し、所定の変換則4を用いて第二の認証用番号を第三の認証用番号に変換し、この第三の認証用番号を新たな第一の認証用番号とする機能とを有する。仲介側情報処理部7は、ユーザ側情報処理部2から送信された第一の認証用番号を認証側情報処理部3へ送信する機能と、認証側情報処理部3から第二の認証用番号を受信し、第二の認

証用番号をユーザ側情報処理部 2 へ送信する機能とを有する。認証側情報処理部 3 は、仲介側情報処理部 7 から第一の認証用番号を受信すると、データベース 5 を用いて照合処理を実行し、この照合処理によって正規ユーザであると認証すると、第一の認証用番号とは異なる第二の認証用番号を仲介側情報処理部 7 へ送信する機能と、変換則 4 と同じものを用いて第二の認証用番号を第三の認証用番号に変換し、第三の認証用番号を新たな第一の認証用番号としてデータベース 5 に記録する機能とを有する。

【 0 0 2 6 】

まず、ユーザ側情報処理部 2 は、第一の認証用番号を仲介側情報処理部 7 へ送信する（ステップ 1 4 0）。仲介側情報処理部 7 は、第一の認証用番号を認証側情報処理部 3 へ送信する（ステップ 1 4 1）。認証側情報処理部 3 は、第一の認証用番号を受信すると、データベース 5 を用いて照合処理を実行する（ステップ 1 4 2）。そして、この照合処理によって正規ユーザであると認証すると、第二の認証用番号を仲介側情報処理部 7 へ送信する（ステップ 1 4 3）。続いて、変換則 4 を用いて第二の認証用番号を第三の認証用番号に変換し（ステップ 1 4 4）、第三の認証用番号を新たな第一の認証用番号としてデータベース 5 に記録する（ステップ 1 4 5）。一方、仲介側情報処理部 7 は、第二の認証用番号をユーザ側情報処理部 2 へ送信する（ステップ 1 4 6）。ユーザ側情報処理部 2 は、第二の認証用番号を受信すると、変換則 4 を用いて第二の認証用番号を第三の認証用番号に変換し、第三の認証用番号を新たな第一の認証用番号とする（ステップ 1 4 7）。なお、ステップ 1 4 2 の照合処理において正規ユーザであると認められない場合は、その後の処理が実行されない。

【 0 0 2 7 】

ここで、例えば通信ネットワーク 1 又は仲介側情報処理部 7 を介して、正規ユーザ以外の第三者によって第一又は第二の認証用番号が知られてしまったとする。そして、その第三者が第一又は第二の認証用番号を使って認証側情報処理部 3 に対するアクセスを試みたとする。しかし、認証側情報処理部 3 では、第一及び第二の認証用番号が既に変換されているので、そのアクセスが許可されることはない。したがって、「なりすまし」による不当なアクセスが防止される。また、

ユーザ側情報処理部 2 では、認証側情報処理部 2 と同じ変換則によって第二の認証用番号が第三の認証用番号に変換されているので、第三の認証用番号を使って認証側情報処理部 2 へアクセスすることができる。

【 0 0 2 8 】

請求項 5 記載のユーザ認証装置は、請求項 1 記載のユーザ認証装置に仲介側情報処理部 7 が付設されたものである。仲介側情報処理部 7 は、例えばサーバー用コンピュータ、パーソナルコンピュータ等である。仲介側情報処理部 7 でも認証用番号が漏洩するおそれがあるので、第一の認証用番号の他にダミー（替え玉）となる第二の認証用番号を使用している。

【 0 0 2 9 】

請求項 5 記載のユーザ認証装置の場合も、請求項 2 乃至 4 記載のユーザ認証装置と同様に、ユーザ側情報処理部に携帯型記録媒体を具備させたものとしてすることができる。それらを請求項 6 乃至 8 記載のユーザ認証装置として、次に示す。

【 0 0 3 0 】

図 6 は請求項 6 記載のユーザ認証装置を示し、図 6 [1] はブロック図、図 6 [2] はシーケンス図である。以下、この図面に基づき説明する。

【 0 0 3 1 】

請求項 6 記載のユーザ認証装置は、ユーザ側情報処理部 2 が携帯型記録媒体 6 を備えている。ユーザ側情報処理部 2 は、携帯型記録媒体 6 から第一の認証用番号及び所定の変換則 4 を読み取り第一の認証用番号を仲介側情報処理部 7 へ送信する機能と、第二の認証用番号を受信すると、変換則 4 を用いて第二の認証用番号を第三の認証用番号に変換し、第二の認証用番号を新たな第一の認証用番号として携帯型記録媒体 6 に記録する機能とを有する。

【 0 0 3 2 】

まず、ユーザ側情報処理部 2 は、携帯型記録媒体 6 から第一の認証用番号及び所定の変換則 4 を読み取り（ステップ 1 5 0, 1 5 1）、第一の認証用番号を仲介側情報処理部 7 へ送信する（ステップ 1 4 0）。仲介側情報処理部 7 は、第一の認証用番号を認証側情報処理部 3 へ送信する（ステップ 1 4 1）。認証側情報処理部 3 は、第一の認証用番号を受信すると、データベース 5 を用いて照合処理

を実行する（ステップ142）。そして、この照合処理によって正規ユーザであると認証すると、第二の認証用番号を仲介側情報処理部7へ送信する（ステップ143）。続いて、変換則4を用いて第二の認証用番号を第三の認証用番号に変換し（ステップ144）、第三の認証用番号を新たな第一の認証用番号としてデータベース5に記録する（ステップ145）。一方、仲介側情報処理部7は、第二の認証用番号をユーザ側情報処理部2へ送信する（ステップ146）。ユーザ側情報処理部2は、第二の認証用番号を受信すると、変換則4を用いて第二の認証用番号を第三の認証用番号に変換し（ステップ147）、第三の認証用番号を新たな第一の認証用番号として携帯型記録媒体6に記録する（ステップ152, 153）。

【0033】

請求項6記載のユーザ認証装置も、請求項5記載のユーザ認証装置と同等の作用及び効果を奏する。携帯型記録媒体6としては、認証用番号及び変換則の記録ができるだけの少ないメモリ容量でよいので、磁気カードが適している。この場合、ユーザ側情報処理部2は、カードリーダー・ライタを備えたものとなる。

【0034】

図7は請求項7記載のユーザ認証装置を示し、図7[1]はブロック図、図7[2]はシーケンス図である。以下、この図面に基づき説明する。

【0035】

請求項7記載のユーザ認証装置は、ユーザ側情報処理部2が携帯型記録媒体6を備えたものである。ユーザ側情報処理部2は、携帯型記録媒体6から第一の認証用番号を読み取り、第一の認証用番号を仲介側情報処理部7へ送信する機能を有する。携帯型記録媒体6、第二の認証用番号を受信されると、所定の変換則4を用いて第二の認証用番号を第三の認証用番号に変換し、第三の認証用番号を新たな第一の認証用番号として携帯型記録媒体6に記録する機能を有する。

【0036】

まず、ユーザ側情報処理部2は、携帯型記録媒体6から第一の認証用番号を読み取り（ステップ160, 161）、第一の認証用番号を仲介側情報処理部7へ送信する（ステップ140）。仲介側情報処理部7は、第一の認証用番号を認証

側情報処理部 3 へ送信する（ステップ 1 4 1）。認証側情報処理部 3 は、第一の認証用番号を受信すると、データベース 5 を用いて照合処理を実行する（ステップ 1 4 2）。そして、この照合処理によって正規ユーザであると認証すると、第二の認証用番号を仲介側情報処理部 7 へ送信する（ステップ 1 4 3）。続いて、変換則 4 を用いて第二の認証用番号を第三の認証用番号に変換し（ステップ 1 4 4）、第三の認証用番号を新たな第一の認証用番号としてデータベース 5 に記録する（ステップ 1 4 5）。一方、仲介側情報処理部 7 は、第二の認証用番号をユーザ側情報処理部 2 へ送信する（ステップ 1 4 6）。ユーザ側情報処理部 2 が第二の認証用番号を受信すると（ステップ 1 6 2）、携帯型記録媒体 6 は、変換則 4 を用いて第二の認証用番号を第三の認証用番号に変換し（ステップ 1 6 3）、第三の認証用番号を新たな第一の認証用番号として携帯型記録媒体 6 に記録する（ステップ 1 6 4）。

【 0 0 3 7 】

請求項 7 記載のユーザ認証装置も、請求項 5 記載のユーザ認証装置と同等の作用及び効果を奏する。携帯型記録媒体 6 としては、認証用番号を変換する演算機能が必要になるので、IC カードが適している。この場合、ユーザ側情報処理部 2 は、IC カードコネクタを備えたものとなる。

【 0 0 3 8 】

図 8 は請求項 8 記載のユーザ認証装置を示し、図 8 [1] はブロック図、図 8 [2] はシーケンス図である。以下、この図面に基づき説明する。

【 0 0 3 9 】

請求項 8 記載のユーザ認証装置は、ユーザ側情報処理部 2 が携帯型記録媒体 6 を備えたものである。ユーザ側情報処理部 2 は、第一の認証用番号を入力して第一の認証用番号を仲介側情報処理部 7 へ送信する機能と、携帯型記録媒体 6 から所定の変換則 4 を読み取るとともに、第二の認証用番号を受信すると、変換則 4 を用いて第二の認証用番号を第三の認証用番号に変換し、第三の認証用番号を新たな第一の認証用番号として出力する機能とを有する。

【 0 0 4 0 】

まず、ユーザ側情報処理部 2 は、第一の認証用番号を入力し（ステップ 1 7 0

）、第一の認証用番号を仲介側情報処理部 7 へ送信する（ステップ 1 4 0）。仲介側情報処理部 7 は、第一の認証用番号を認証側情報処理部 3 へ送信する（ステップ 1 4 1）。認証側情報処理部 3 は、第一の認証用番号を受信すると、データベース 5 を用いて照合処理を実行する（ステップ 1 4 2）。そして、この照合処理によって正規ユーザであると認証すると、第二の認証用番号を仲介側情報処理部 7 へ送信する（ステップ 1 4 3）。続いて、変換則 4 を用いて第二の認証用番号を第三の認証用番号に変換し（ステップ 1 4 4）、第三の認証用番号を新たな第一の認証用番号としてデータベース 5 に記録する（ステップ 1 4 5）。一方、仲介側情報処理部 7 は、第二の認証用番号をユーザ側情報処理部 2 へ送信する（ステップ 1 4 6）。ユーザ側情報処理部 2 は、第二の認証用番号を受信すると携帯型記録媒体 6 から所定の変換則 4 を読み取り（ステップ 1 7 1, 1 7 2）、変換則 4 を用いて第二の認証用番号を第三の認証用番号に変換し（ステップ 1 7 3）、第三の認証用番号を新たな第一の認証用番号として出力する（ステップ 1 7 4）。

【 0 0 4 1 】

請求項 8 記載のユーザ認証装置も、請求項 5 記載のユーザ認証装置と同等の作用及び効果を奏する。ステップ 1 7 0 における第一の認証用番号の入力は、例えばユーザによるキーボードからの入力である。ステップ 1 7 4 における新たな第一の認証用番号の出力は、例えばユーザだけが見ることのできるディスプレイへの表示である。携帯型記録媒体 6 としては、変換則の記録ができるだけの少ないメモリ容量でよいので、磁気カードが適している。認証用番号としては、携帯型記録媒体 6 に記録されないので、暗証番号が適している。なお、ユーザ側情報処理部 2 に変換則が記録されていれば、携帯型記録媒体 6 が不要になるが、この場合の構成は請求項 5 記載のユーザ認証装置に含まれる。

【 0 0 4 2 】

請求項 9 記載の商取引システムは、請求項 2 又は 3 記載のユーザ認証装置を用いたものである。以下、図 2 及び図 3 に基づき説明する。

【 0 0 4 3 】

ユーザ側情報処理部 2 は、第一の認証用番号とともに決済要求を認証側情報処

理部 3 へ送信する。認証側情報処理部 3 は、照合処理とともに決済処理を実行する。そして、通信ネットワーク 1 がインターネット、ユーザ側情報処理部 2 が店頭端末、認証側情報処理部 3 がクレジット会社端末、携帯型記録媒体 6 がクレジットカード、認証用番号がクレジット番号である。

【0044】

請求項 10 記載の商取引システムは、請求項 4 記載のユーザ認証装置を用いたものである。以下、図 4 に基づき説明する。

【0045】

ユーザ側情報処理部 2 は、第一の認証用番号とともに決済要求を認証側情報処理部へ送信する。認証側情報処理部 3 は、照合処理とともに決済処理を実行する。そして、通信ネットワーク 1 がインターネット、ユーザ側情報処理部 2 が店頭端末、認証側情報処理部 3 が銀行端末、携帯型記録媒体 6 がキャッシュカード、認証用番号が暗証番号である。

【0046】

請求項 11 記載の商取引システムは、請求項 6 又は 7 記載のユーザ認証装置を用いたものである。以下、図 6 又は図 7 に基づき説明する。

【0047】

仲介側情報処理部 7 は、第一の認証用番号とともに決済要求を認証側情報処理部 3 へ送信する。認証側情報処理部 3 は、照合処理とともに決済処理を実行する。そして、通信ネットワーク 1 がインターネット、ユーザ側情報処理部 2 がユーザ端末、仲介側情報処理部 7 が販売センター端末、認証側情報処理部 3 がクレジット会社端末、携帯型記録媒体 6 がクレジットカード、認証用番号がクレジット番号である。

【0048】

請求項 12 記載の商取引システムは、請求項 8 記載のユーザ認証装置を用いたものである。以下、図 8 に基づき説明する。

【0049】

仲介側情報処理部 7 は、第一の認証用番号とともに決済要求を認証側情報処理部 3 へ送信する。認証側情報処理部 3 は、照合処理とともに決済処理を実行する

。そして、通信ネットワーク 1 がインターネット、ユーザ側情報処理部 2 がユーザ端末、仲介側情報処理部 7 が販売センター端末、認証側情報処理部 3 が銀行端末、携帯型記録媒体 6 がキャッシュカード、認証用番号が暗証番号である。

【 0 0 5 0 】

以上のとおり、本発明は、インターネット上における商取引においてクレジットカード等による決済を利用した場合に、取引後、クレジットカード番号等をローカルに変換することにより、万一、ネットワーク上でクレジットカード番号等が盗まれた場合でも悪用されるのを防ぐことができるビジネスモデルを提供するものである。

【 0 0 5 1 】

【発明の実施の形態】

図 9 は、本発明に係る商取引システムの第一実施形態を示すブロック図である。以下、この図面に基づき説明する。

【 0 0 5 2 】

ユーザ側情報処理部 2 は、カードリーダー・ライター 2 0 及びクレジットカード 2 5 が付設されたユーザ端末 1 0 からなる。仲介側情報処理部 7 は、販売センター端末 3 0 からなる。認証側情報処理部 3 は、顧客データベース 5 0 が付設されたクレジットカード会社端末 4 0 からなる。

【 0 0 5 3 】

注文者は、販売センター端末 3 0 に対し、ユーザ端末 1 0 を用いて商品の注文を行う。このとき、ユーザ端末 1 0 は、カードリーダー・ライター 2 0 を介してクレジットカード 2 5 にアクセスし、記録されているクレジットカード番号を読み取り同時に送出する。販売センター 3 0 は、送出されたクレジットカード番号に対する決済の要求を、クレジットカード会社端末 4 0 へ行う。クレジットカード会社端末 4 0 は、決済の要求を受け取ると、顧客データベース 5 0 にアクセスして決済の処理を行う。決済完了後、その旨を知らせる通知と新しいクレジットカード番号とを、販売センター端末 3 0 へ送出する。販売センター端末 3 0 は、通知を受け取ると、取引が完了したことを示す通知と新しいクレジットカード番号とを、ユーザ端末 1 0 へ送出する。ユーザ端末 1 0 は、新しいクレジットカード番号を受け取ると、クレジットカード 2 5 に記録されている変換則を用いてクレジットカード番号を変換したのち、それをクレジットカード

ード25に記録する。一方、顧客データベース50も、顧客データベース50内に記録されている同じ変換則を用いて新しいクレジット番号を変換したのち、それを顧客データベース50内に記録する。次の取り引きには、変換されたクレジット番号が用いられる。

【0054】

つまり、本実施形態の商取引システムは、ユーザ端末10、ユーザ端末10にローカルに接続されたカードリーダー・ライター20、カードリーダー・ライター20に挿入されるクレジットカード25、販売センター端末30、クレジット会社端末40、クレジット会社端末40にローカルに接続された顧客データベース50、ユーザ端末10・販売センター端末30・クレジット会社端末40を相互に接続する通信ネットワークとしてのインターネット100等を備えている。

【0055】

ユーザ端末10は、パーソナルコンピュータ等の情報処理装置である。ユーザ端末10は、インターネット100を介して販売センター端末30へアクセスし、販売センター端末30との間で情報を送受信する機能を有する。また、受信した情報などを画面に表示する画面出力機能、注文者が購入希望商品を選択したり、住所等の情報を入力するための入力機能等を有する。また、カードリーダー・ライター20を介してクレジットカード25から情報を読み取る機能、カードリーダー・ライター20を介してクレジットカード25へ情報を記録する機能等を有する。その他、クレジットカード25から読み取った変換則を用いて、クレジット番号を変換する機能を有する。

【0056】

カードリーダー・ライター20は、クレジットカード25へ情報を読み書きするための装置であり、ユーザ端末10にローカルに接続されている。カードリーダー・ライター20は、ユーザ端末10からの読み取り要求に対し、クレジットカード25から情報を読み取り、ユーザ端末10へ送出する機能を有する。また、ユーザ端末10からの書き込み要求に対し、ユーザ端末10から受け取った情報をクレジットカード25へ書き込む機能を有する。

【0057】

クレジットカード25は、クレジット会社から注文者へ提供された固有情報が記録された媒体である。クレジットカード25は、注文者がクレジット会社と契約する際に作成され、情報が記録されたのち注文者に手渡し又は郵送等により提供される。記録されている情報は、クレジット番号及びクレジット番号変換則である。クレジット番号はカードリーダー・ライター20による読み取り及び書き込みが可能であり、クレジット番号変換則は読み取りのみ可能である。クレジットカード25は、カードリーダー・ライター20に挿入されており、読み書きが可能な状態であるものとする。

【0058】

販売センター端末30は、ワークステーション・サーバ等の情報処理装置である。販売センター端末30は、インターネット100を介してユーザ端末10及びクレジット会社端末40との間で情報を送受信する機能を有する。また、受信した注文情報から金額を算出する機能、商品発送等の処理を行う機能などを有する。

【0059】

クレジット会社端末40は、パーソナルコンピュータ等の情報処理装置である。クレジット会社端末40は、インターネット100を介して販売センター端末30との間で情報を送受信する機能、ローカルに接続された顧客データベース50と情報を送受信する機能等を有する。

【0060】

顧客データベース50は、ワークステーション・サーバ等の情報処理装置である。顧客データベース50には、顧客に関する情報が記録されている。記録されている情報は、クレジット番号、氏名等の個人情報、及びクレジット番号変換則である。クレジット番号及びクレジット番号変換則は、クレジットカード25に記録されているものと同じである。顧客データベース50は、クレジット会社端末40とローカルに接続され、クレジット会社端末40との間で情報を送受信する機能を有する。また、クレジット番号及び取引金額等を照合する機能、新しいクレジット番号を生成する機能等を有する。更に、顧客データベース50内に記録されているクレジット番号変換則を用いてクレジット番号を変換する機能、変

換後のクレジット番号を顧客データベース50内に記録する機能等を有する。

【0061】

図10乃至12は、本実施形態の商取引システムの動作を示すシーケンス図である。図13はユーザ端末の表示画面であり、図13[1]は第一例、図13[2]は第二例である。以下、図9乃至図13に基づき、本実施形態の商取引システムの動作を説明する。

【0062】

ユーザ端末10-販売センター端末30間、及び販売センター端末30-クレジット会社端末40間のデータ送受信は、インターネット100を介して行われるものとする。ユーザ端末10-カードリーダー・ライタ20-クレジットカード25間、及びクレジット会社端末40-顧客データベース50間のデータ送受信は、ローカルに行われるものとする。

【0063】

まず、注文者は、自分のユーザ端末10を用いて、販売センターがインターネット100上に開設している製品販売ホームページにアクセスする(図10ステップA1)。これに応答して、販売センター端末30は商品情報をユーザ端末10に送信する(図10ステップA2)。商品情報を受信後、ユーザ端末10には、図13[1]に示すような商品情報が表示される(図10ステップA3)。注文者は、ユーザ端末10の画面に表示された商品情報を見て、購入したい商品を決して、その商品を購入する旨を画面上で登録する(図10ステップA4)。図13[1]の例では、注文者が商品Bの購入欄をマウスでクリックすると、レ印が付けられ、この商品Bが購入登録されている。こうして登録された、注文者が購入する商品の商品情報は、一時的にユーザ端末10に蓄えられる。

【0064】

続いて、注文者が図13[1]の画面上の「購入」ボタンをマウスでクリックすると、ユーザ端末10には、図13[2]に示すような、商品を購入するのに必要な情報を入力するための入力フォームが画面上に表示される(図10ステップA5)。注文者は購入希望商品の確認を行ったのち、各種情報を入力する(図10ステップA6)。入力する情報は、注文者の住所(商品の配送先)、氏名、

電話番号等の個人情報及び支払方法である。図13[2]の例では、注文者がクレジットカード25による支払いのチェック欄をクリックし、本発明が提案するクレジットカード25による支払いを選択したことを示している。これらの情報は一時的にユーザ端末10に蓄えられる。

【0065】

続いて、注文者が図13[2]の画面上の「送信」ボタンをマウスでクリックすると、ユーザ端末10は、クレジットカード25にアクセスし（図10ステップA7）、クレジットカード25に記録されているクレジット番号を読み取る（図10ステップA8）。ここでは一例として、クレジットカード25にはクレジット番号1234が記録されているものとする。ユーザ端末10は、クレジットカード25からクレジット番号1234を受け取ると、ユーザ端末10に蓄えられていた購入商品情報、個人情報及び支払方法と、読み取ったクレジット番号1234とをまとめて商品注文情報として、販売センター端末30へ送出する（図10ステップA9）。

【0066】

販売センター端末30は、商品注文情報を受け取ると（図10ステップA10）、購入商品情報から金額の合計を算出する（図10ステップA11）。その後、クレジットカード25による決済を行うために、注文者の個人情報、クレジットカード番号1234、取引金額、及び代金の振込先（販売センターの口座番号など）をまとめて取引情報として、クレジット会社端末40へ送出する（図10ステップA12）。

【0067】

クレジット会社端末40は、取引情報を受け取ると（図11ステップA13）、その情報を顧客データベース50へ送出し（図11ステップA14）、取引の確認を行う。

【0068】

顧客データベース50は、取引情報を受け取ると（図11ステップA15）、個人情報及びクレジット番号から注文者の照合を行う（図11ステップA16）。情報に誤りがある場合には、クレジット会社端末40→販売センター端末30

→ユーザ端末10を介して、注文者にその旨を知らせる。注文者照合の終了後、顧客データベース50は、取引金額の照合を行う（図11ステップA17）。取引金額がクレジットカード25の利用限度額を越えている場合等、取引が行えない場合には、クレジット会社端末40→販売センター端末30→ユーザ端末10を介して、注文者にその旨を知らせる。取引に問題がないことが確認できれば、顧客データベース50は決済の処理を行う（図11ステップA18）。決済の処理を行ったのち、顧客データベース50は新しいクレジット番号を生成する（図11ステップA19）。ここでは一例として、クレジット番号5678を生成したものとする。

【0069】

顧客データベース50は、決済が完了したことを示す決済完了情報と、新しく生成したクレジット番号5678とを、クレジット会社端末40へ送付する（図11ステップA20）。その後、顧客データベース50は、顧客データベース50に記録されているクレジットカード25の変換則（ここでは一例として、クレジット番号に1111を加えるものとする。）を呼び出し（図11ステップB21）、これを用いて先ほど生成した新しいクレジット番号5678を6789に変換し（図11ステップB22）、変換後のクレジット番号6789を顧客データベース50内に記録する（図11ステップB23）。

【0070】

クレジット会社端末40は、決済完了情報と新しいクレジット番号5678とを受け取ると（図11ステップA21）、それらを販売センター端末30へ送付する（図11ステップA22）。

【0071】

販売センター端末30は、決済完了情報と新しいクレジット番号5678とを受け取ると（図12ステップA23）、商品発送の処理を行う（図12ステップA24）。その後、取引が完了したことを示す取引完了通知と新クレジット番号5678とを、ユーザ端末10へ送付する（図12ステップA25）。

【0072】

ユーザ端末10は、取引完了通知及び新クレジット番号5678を受け取ると、ク

クレジットカード25にアクセスし（図12ステップA27）、記録されている変換則（ $x=x+1111$ ）を読み取る（図12ステップA28）。この変換則を用いて、新クレジットカード番号5678を6789に変換し（図12ステップA29）、クレジットカード25へ送出したのち（図12ステップA30）、クレジットカード25に記録する（図12ステップA31）。変換後のクレジットカード番号の記録が完了後（図12ステップA32）、ユーザ端末10は、取引が完了したことを画面に表示することにより（図12ステップA33）、注文者に取引が完了したことを示す。

【0073】

図14乃至16は、本発明に係る商取引システムの第二実施形態の動作を示すシーケンス図である。以下、図13乃至図16に基づき、本実施形態の商取引システムを説明する。

【0074】

本実施形態の商取引システムでは、第一実施形態におけるクレジットカード25及びクレジット会社端末40の代わりに、キャッシュカード26及び銀行端末41となっている。キャッシュカード26は、銀行が注文者に対して提供する、固有情報が記録された媒体である。キャッシュカード26に記録されている情報は、注文者の口座番号及び暗証番号変換則とする。キャッシュカード26による決済を行う場合、暗証番号による照合を行うが、取り引き後に暗証番号を変換することにより、インターネット100上で暗証番号が盗まれた場合でも悪用されることを防ぐ。

【0075】

暗証番号は、注文者による手入力を行うため、キャッシュカード26に書き込まない。そのため、キャッシュカード26は読み取り専用でよい。また、カードリーダー・ライタ20も読み取り機能のみでよい。ただし、クレジットカード25のように、暗証番号をキャッシュカード26から読み取るようにしてもよい。

【0076】

まず、注文者は、自分のユーザ端末10を用いて、販売センターがインターネット100上に開設している製品販売ホームページにアクセスする（図14ステ

ップA1)。これに応答して、販売センター端末30は商品情報をユーザ端末10に送信する(図14ステップA2)。商品情報を受信後、ユーザ端末10には、図13[1]に示すような商品情報が表示される(図14ステップA3)。注文者は、ユーザ端末10の画面に表示された商品情報を見て、購入したい商品を決定して、その商品を購入する旨を画面上で登録する(図14ステップA4)。図13[1]の例では、注文者が商品Bの購入欄をマウスでクリックすると、レ印が付けられ、この商品Bが購入登録されている。こうして登録された、注文者が購入する商品の商品情報は、一時的にユーザ端末10に蓄えられる。

【0077】

続いて、注文者が図13[1]の画面上の「購入」ボタンをマウスでクリックすると、ユーザ端末10には、図13[2]に示すような、商品を購入するのに必要な情報を入力するための入力フォームが画面上に表示される(図14ステップA5)。注文者は購入希望商品の確認を行ったのち、各種情報を入力する(図14ステップA6)。入力する情報は、注文者の住所(商品の配送先)、氏名、電話番号等の個人情報、支払方法及び暗証番号である。図13[2]の例では、注文者が、キャッシュカード26(銀行カード)による支払いのチェック欄をクリックし、暗証番号(ここでは一例として1234とする。)等をキーボードから入力する。これらの情報は一時的にユーザ端末10に蓄えられる。

【0078】

続いて、注文者が図13[2]の画面上の「送信」ボタンをマウスでクリックすると、ユーザ端末10は、キャッシュカード26にアクセスし(図14ステップA7)、キャッシュカード26に記録されている口座番号を読み取る(図14ステップA8)。ユーザ端末10は、キャッシュカード26から口座番号を受け取ると、ユーザ端末10に蓄えられていた購入商品情報、個人情報、支払方法及び暗証番号1234と、読み取った口座番号とをまとめて商品注文情報として、販売センター端末30へ送出する(図14ステップA9)。

【0079】

販売センター端末30は、商品注文情報を受取ると(図14ステップA10)、購入商品情報から金額の合計を算出する(図14ステップA11)。その後、

キャッシュカード26による決済を行うために、注文者の個人情報、口座番号、暗証番号1234、取引金額、及び代金の振込先（販売センターの口座番号など）をまとめて取引情報として、銀行端末41へ送出する（図14ステップA12）。

【0080】

銀行端末41は、取引情報を受け取ると（図15ステップA13）、その情報を顧客データベース50へ送出し（図15ステップA14）、取引の確認を行う。

【0081】

顧客データベース50は、取引情報を受け取ると（図15ステップA15）、個人情報及び暗証番号に基づき注文者の照合を行う（図15ステップA16）。情報に誤りがある場合には、銀行端末41→販売センター端末30→ユーザ端末10を介して、注文者にその旨を知らせる。注文者照合の終了後、顧客データベース50は、取引金額の照合を行う（図15ステップA17）。取引金額がキャッシュカード25の残高を越えている場合等、取引が行えない場合には、銀行端末41→販売センター端末30→ユーザ端末10を介して、注文者にその旨を知らせる。取引に問題がないことが確認できれば、顧客データベース50は決済の処理を行う（図15ステップA18）。決済の処理を行ったのち、顧客データベース50は新しい暗証番号を生成する（図15ステップA19）。ここでは一例として、暗証番号5678を生成したものとする。

【0082】

顧客データベース50は、決済が完了したことを示す決済完了情報と、新しく生成した暗証番号5678とを銀行端末41へ送出する（図15ステップA20）。その後、顧客データベース50は、顧客データベース50に記録されているキャッシュカード26の変換則（ここでは一例として、暗証番号に1111を加えるものとする。）を呼び出し（図15ステップB21）、これを用いて先ほど生成した新しい暗証番号5678を6789に変換し（図15ステップB22）、変換後の暗証番号6789を顧客データベース50内に記録する（図15ステップB23）。

【0083】

銀行端末41は、決済完了情報と新しい暗証番号5678とを受け取ると（図15

ステップA21)、それらを販売センター端末30へ送出する(図15ステップA22)。

【0084】

販売センター端末30は、決済完了情報と新しい暗証番号5678とを受け取ると(図16ステップA23)、商品発送の処理を行う(図16ステップA24)。その後、取引が完了したことを示す取引完了通知と新暗証番号5678とを、ユーザ端末10へ送出する(図16ステップA25)。

【0085】

ユーザ端末10は、取引完了通知及び新暗証番号5678を受け取ると、キャッシュカード26にアクセスし(図16ステップA27)、記録されている変換則($x=x+1111$)を読み取る(図16ステップA28)。この変換則を用いて、新暗証番号5678を6789に変換する(図16ステップA29)。最後に、ユーザ端末10は、新暗証番号6789及び取引が完了したことを画面に表示することにより(図16ステップA30)、注文者に取引が完了したことを示す。

【0086】

以上で上記第一及び第二の実施形態の説明を終えるが、本発明は、言うまでもなく、これらの実施形態に限定されるものではない。以下に、他の形態を列挙する。

【0087】

クレジット番号変換則は、通信ネットワーク上を流れるクレジット番号を別のものに変換するものであれば何でもよい。上記実施形態に示したように、関数を用いて変換するようなものでもよいし、ある法則により文字列を別の文字列に置き換えるようなものでもよい。また、それらを複合して使用してもよい。変換則に定数又はキーワードを必要とするものでもよい。キーワードを利用した場合、変換方法を公開又は共通のものとして、キーワードのみカード固有としてもよい。また、新しいクレジット番号を送出せず、現在使用しているクレジット番号を変換則を用いて別のものに変換するという方法でもよい。

【0088】

上記実施形態ではクレジット番号の変換をユーザ端末10にて行っているが、

この変換機能をカードリーダー・ライタ 2 0 に持たせてもよい。また、クレジットカード 2 5 にこの機能を持たせてもよい。同様に顧客データベース 5 0 での変換をクレジット会社端末 4 0 又は銀行端末 4 1 にて行ってもよい。

【 0 0 8 9 】

本発明は、クレジット番号や暗証番号以外の I D 番号、パスワード等の保護にも使用できる。例えば、会員制の W e b サイトにおいて、パスワードによる区別を行うような場合、パスワードを変換則を用いて変換することにより、ネットワーク上でパスワードを盗まれた場合でも悪用を防ぐことができる。

【 0 0 9 0 】

ユーザ端末 1 0 は、個人が使用するものでなくてもよい。例えば、公共機関等に設置された、複数の人間が共通で使用するような端末でもよい。

【 0 0 9 1 】

本発明はネットワーク上ではなく、店頭販売されている商品を購入する場合にも適用することができる。例えば、支払いの際に店頭に設置された端末を使用するという方法である。この場合、店頭端末－クレジット会社端末（又は銀行端末）間で情報が盗まれた場合の悪用を防ぐことができる。

【 0 0 9 2 】

クレジットカード 2 5 は、インターネット 1 0 0 に接続されたユーザ端末 1 0 にデータを送受信できる、読み書き可能な媒体であれば何でもよい。例えば、磁気記録を用いたクレジットカードの他、I C チップを搭載したものなどでもよい。また、カードである必要もなく、例えばフラッシュ・メモリ・カードなどでもよい。また、フロッピーディスク等、磁気や光などを利用した記録媒体などでもよい。

【 0 0 9 3 】

ユーザ端末 1 0 とカードリーダー・ライタ 2 0 とは、別々である必要はなく、一体化されたものでもよい。また、クレジット会社端末 4 0 （又は銀行端末 4 1 ）と顧客データベース 5 0 とも一体化されたものでもよい。

【 0 0 9 4 】

【発明の効果】

本発明に係るユーザ認証装置によれば、正規ユーザ以外の第三者によって認証用番号が盗まれても、その認証用番号は一回しか使用できないので、「なりすまし」による不当なアクセスを防止できる。また、本発明に係る商取引システムによれば、本発明に係るユーザ認証装置を用いたことにより、ユーザ認識を正確に実行できるので、通信ネットワークを用いた安全な電子商取引を実現できる。

【 0 0 9 5 】

換言すると、本発明は次の四つの効果を奏する。

【 0 0 9 6 】

第1の効果は、通信ネットワーク上を流れるクレジット番号、暗証番号等の認証用番号が第三者に盗まれた場合でも、悪用されることがない点である。その理由は、クレジット番号等は取引の度に新しいものに変更されるため、第三者がクレジット番号を盗んだとしても、その番号を利用することができないためである。

【 0 0 9 7 】

第2の効果は、クレジット番号、暗証番号等の認証用番号の変換則が盗まれないことである。その理由は、クレジット番号等の変換則がクレジットカードに予め記録されていること、及びクレジット番号等の変換がローカルに行われることにより、クレジット番号等の変換に関する情報が通信ネットワーク上に流出しないためである。

【 0 0 9 8 】

第3の効果は、クレジット番号等の入力の煩わしさを除くことができる点である。その理由は、ユーザ端末がクレジットカード等から番号を読み取って送出するため、注文者が改めて入力する必要がないためである。

【 0 0 9 9 】

第4の効果は、クレジット番号等の入力ミスを防ぐことができる点である。その理由は、ユーザ端末がクレジットカード等から番号を読み取って送出するため、注文者が改めて入力する必要がないためである。

【図面の簡単な説明】

【図 1】

図 1 は請求項 1 記載のユーザ認証装置を示し、図 1 [1] はブロック図、図 1 [2] はシーケンス図である。

【図 2】

図 2 は請求項 2 記載のユーザ認証装置を示し、図 2 [1] はブロック図、図 2 [2] はシーケンス図である。

【図 3】

図 3 は請求項 3 記載のユーザ認証装置を示し、図 3 [1] はブロック図、図 3 [2] はシーケンス図である。

【図 4】

図 4 は請求項 4 記載のユーザ認証装置を示し、図 4 [1] はブロック図、図 4 [2] はシーケンス図である。

【図 5】

図 5 は請求項 5 記載のユーザ認証装置を示し、図 5 [1] はブロック図、図 5 [2] はシーケンス図である。

【図 6】

図 6 は請求項 6 記載のユーザ認証装置を示し、図 6 [1] はブロック図、図 6 [2] はシーケンス図である。

【図 7】

図 7 は請求項 7 記載のユーザ認証装置を示し、図 7 [1] はブロック図、図 7 [2] はシーケンス図である。

【図 8】

図 8 は請求項 8 記載のユーザ認証装置を示し、図 8 [1] はブロック図、図 8 [2] はシーケンス図である。

【図 9】

本発明に係る商取引システムの第一実施形態を示すブロック図である。

【図 10】

本発明に係る商取引システムの第一実施形態の動作を示すシーケンス図である。

【図 11】

本発明に係る商取引システムの第一実施形態の動作を示すシーケンス図である

【図 1 2】

本発明に係る商取引システムの第一実施形態の動作を示すシーケンス図である

【図 1 3】

第一実施形態におけるユーザ端末の表示画面であり、図 1 3 [1] は第一例、
図 1 3 [2] は第二例である。

【図 1 4】

本発明に係る商取引システムの第二実施形態の動作を示すシーケンス図である

【図 1 5】

本発明に係る商取引システムの第二実施形態の動作を示すシーケンス図である

【図 1 6】

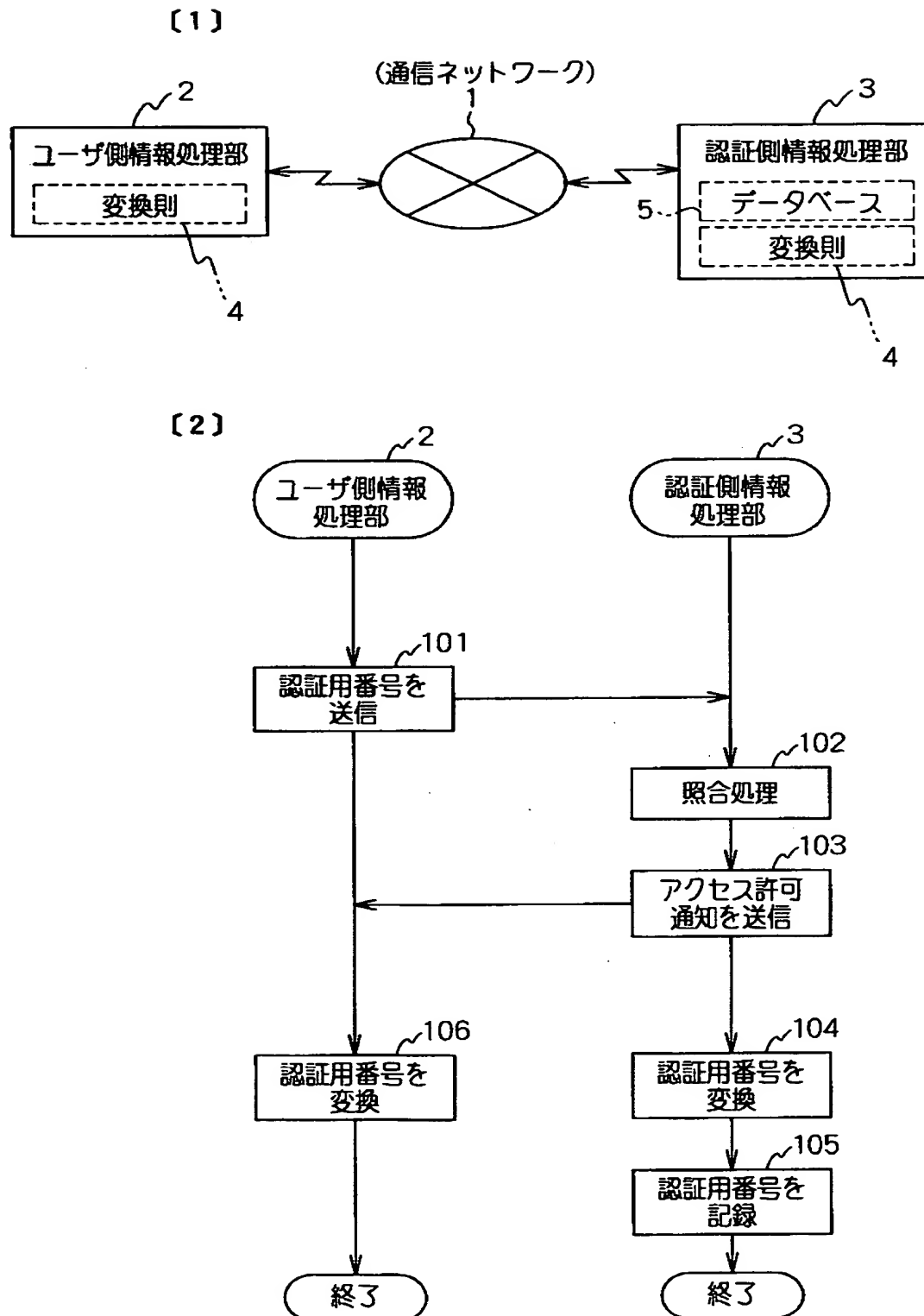
本発明に係る商取引システムの第二実施形態の動作を示すシーケンス図である

【符号の説明】

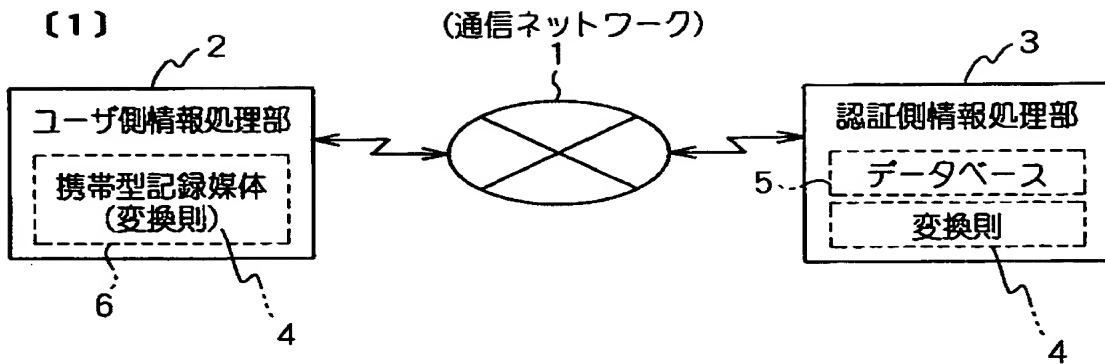
- 1 通信ネットワーク
- 2 ユーザ側情報処理部
- 3 認証側情報処理部
- 4 変換則
- 5 データベース
- 6 携帯型記録媒体
- 7 仲介側情報処理部
- 1 0 ユーザ端末
- 2 0 カードリーダー・ライタ
- 2 5 クレジットカード
- 2 6 キャッシュカード

- 3 0 販売センター端末
- 4 0 クレジット会社端末
- 4 1 銀行端末
- 5 0 顧客データベース

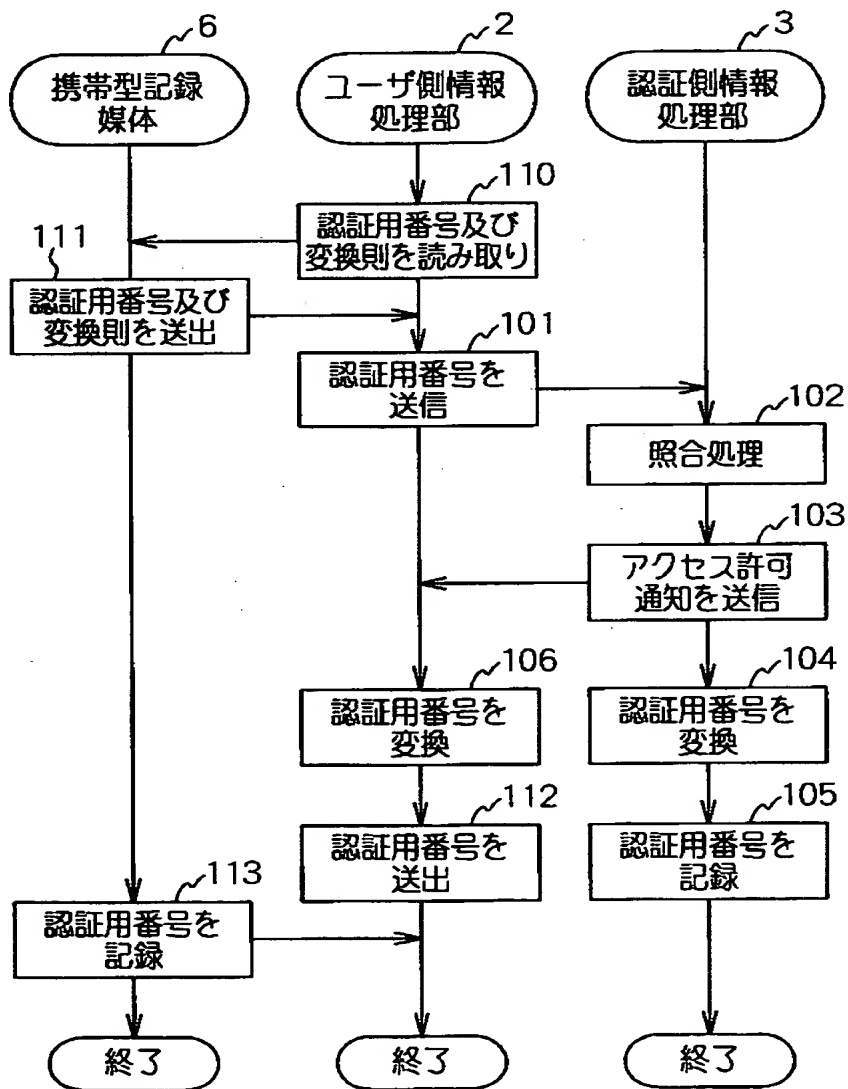
【書類名】 図面
【図1】



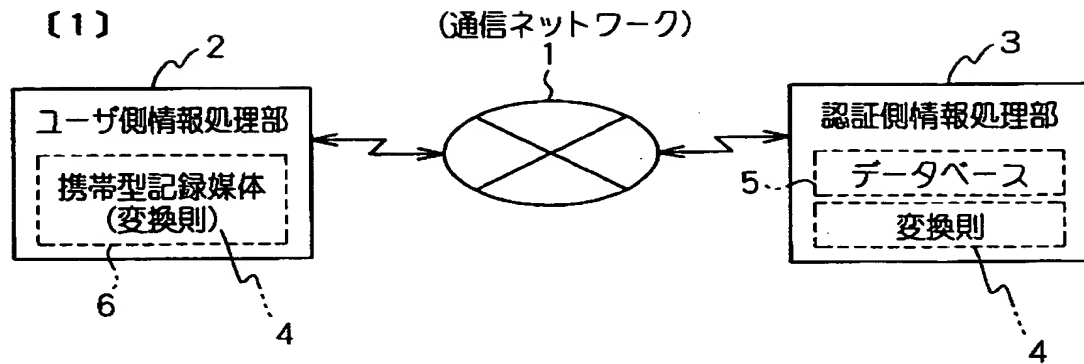
【図 2】



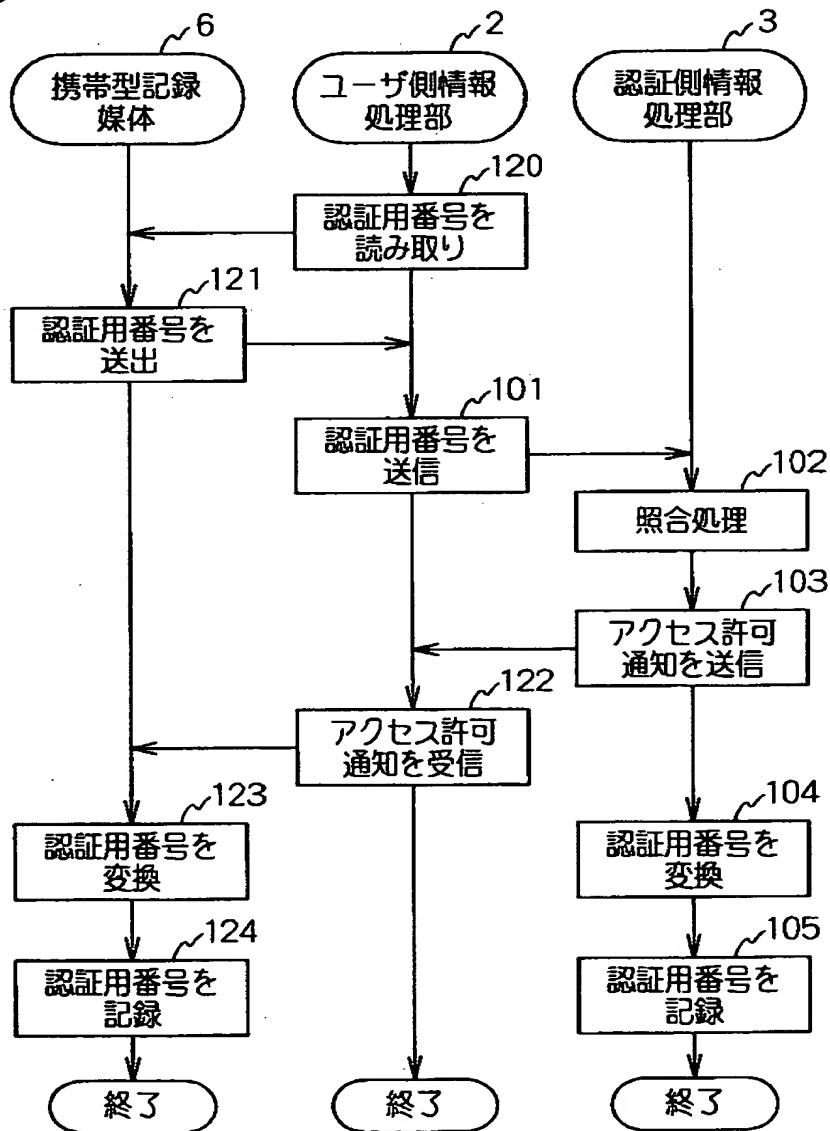
(2)



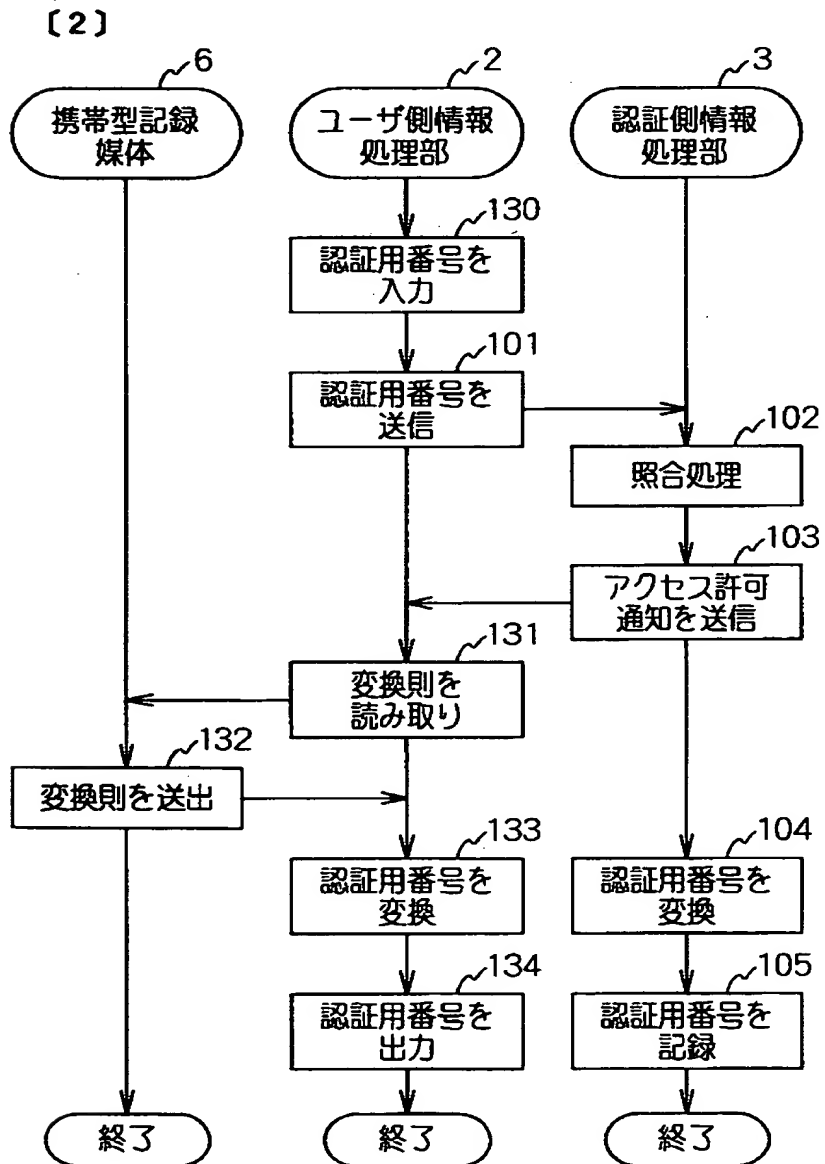
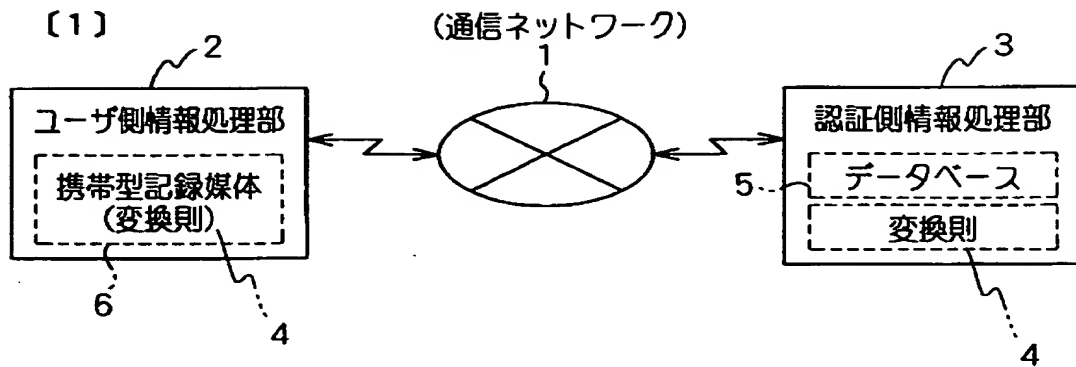
【図3】



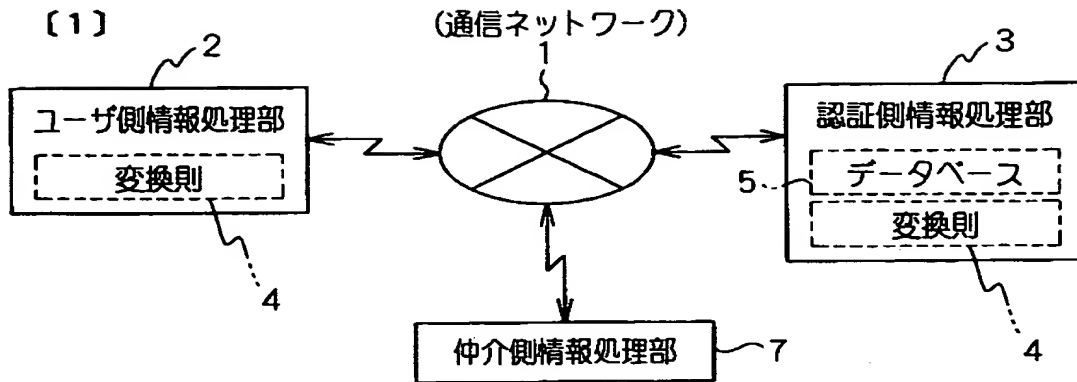
(2)



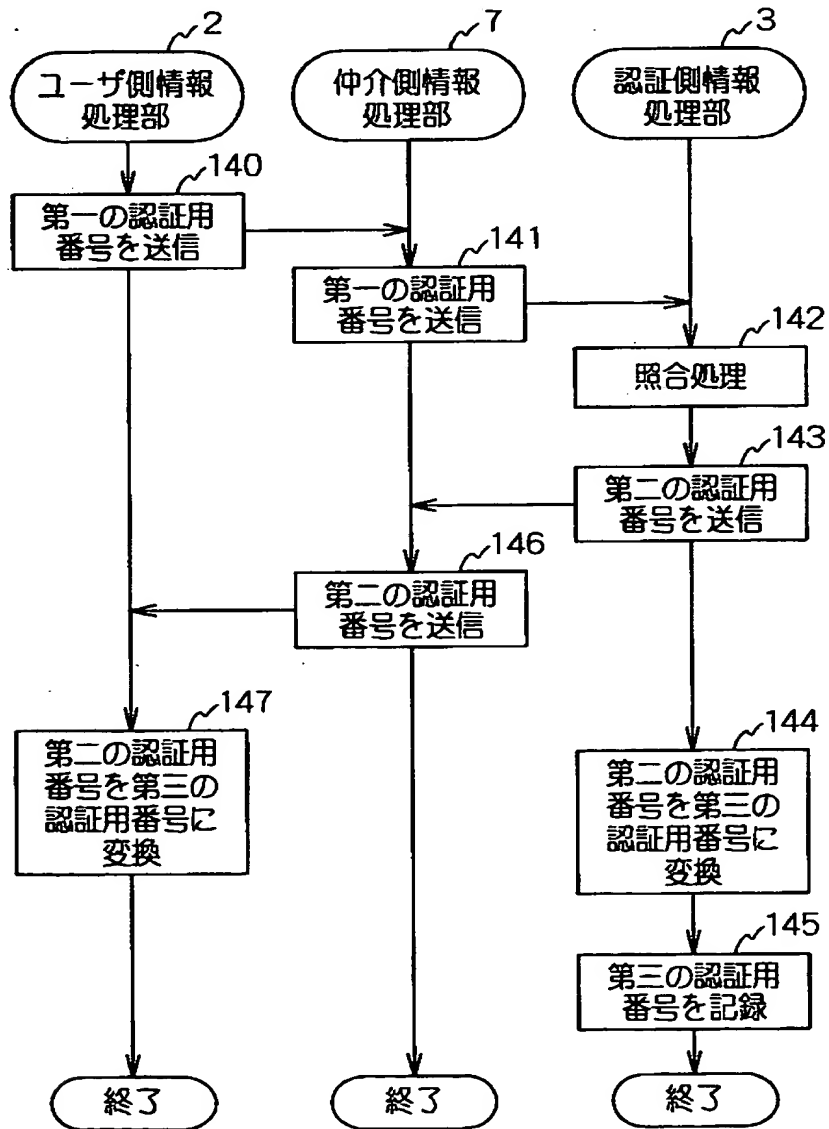
【図 4】



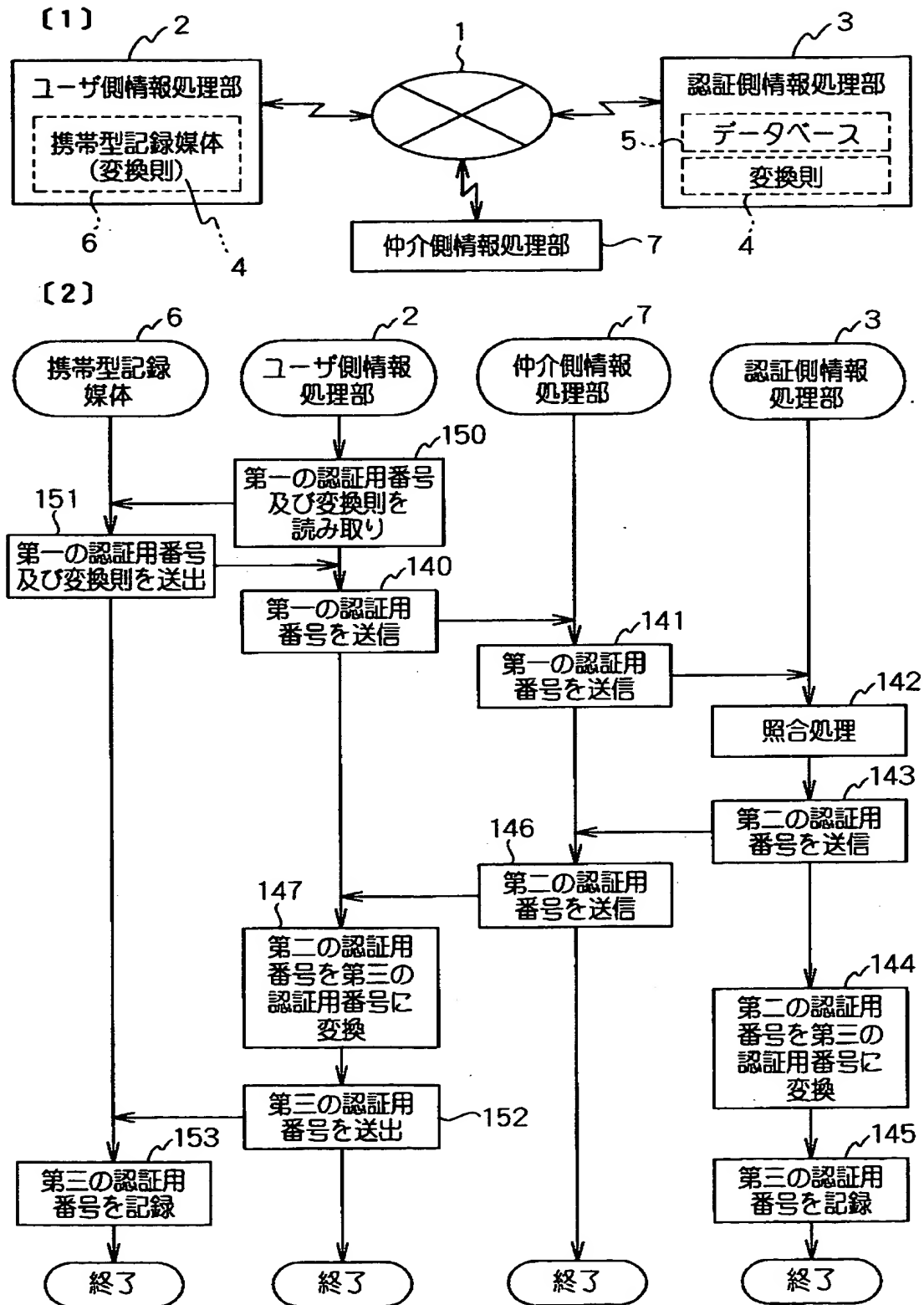
【図5】



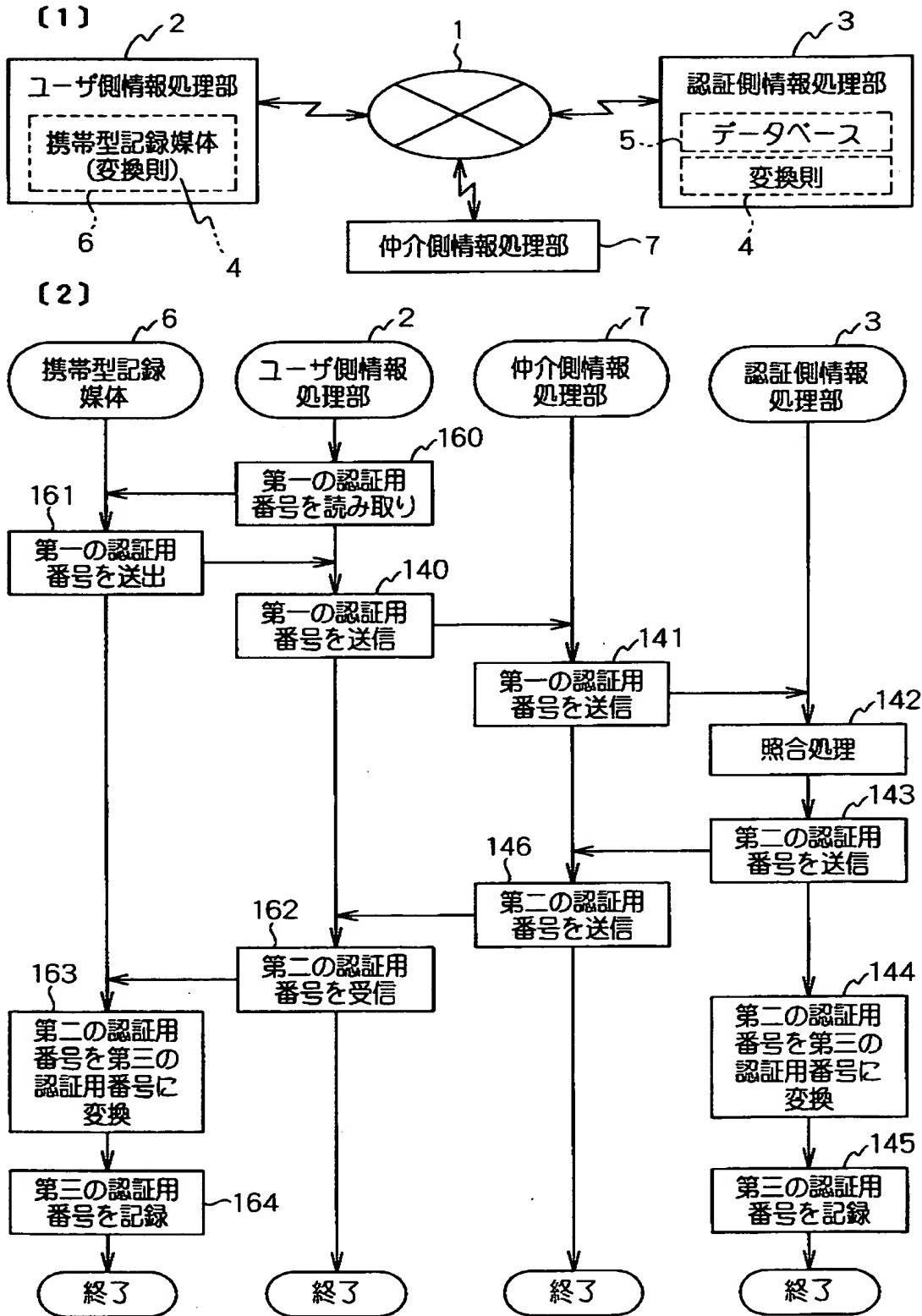
(2)



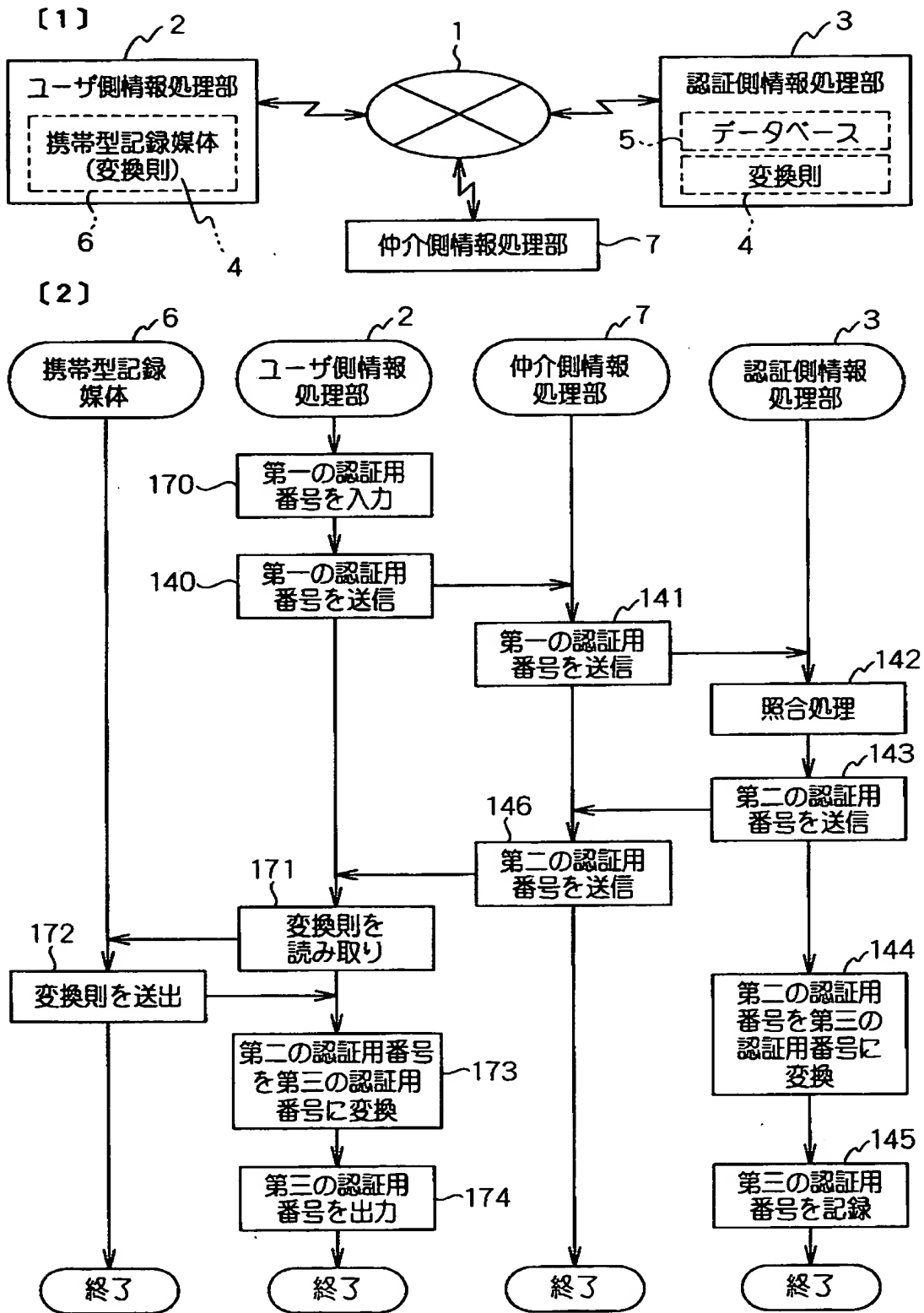
【図 6】



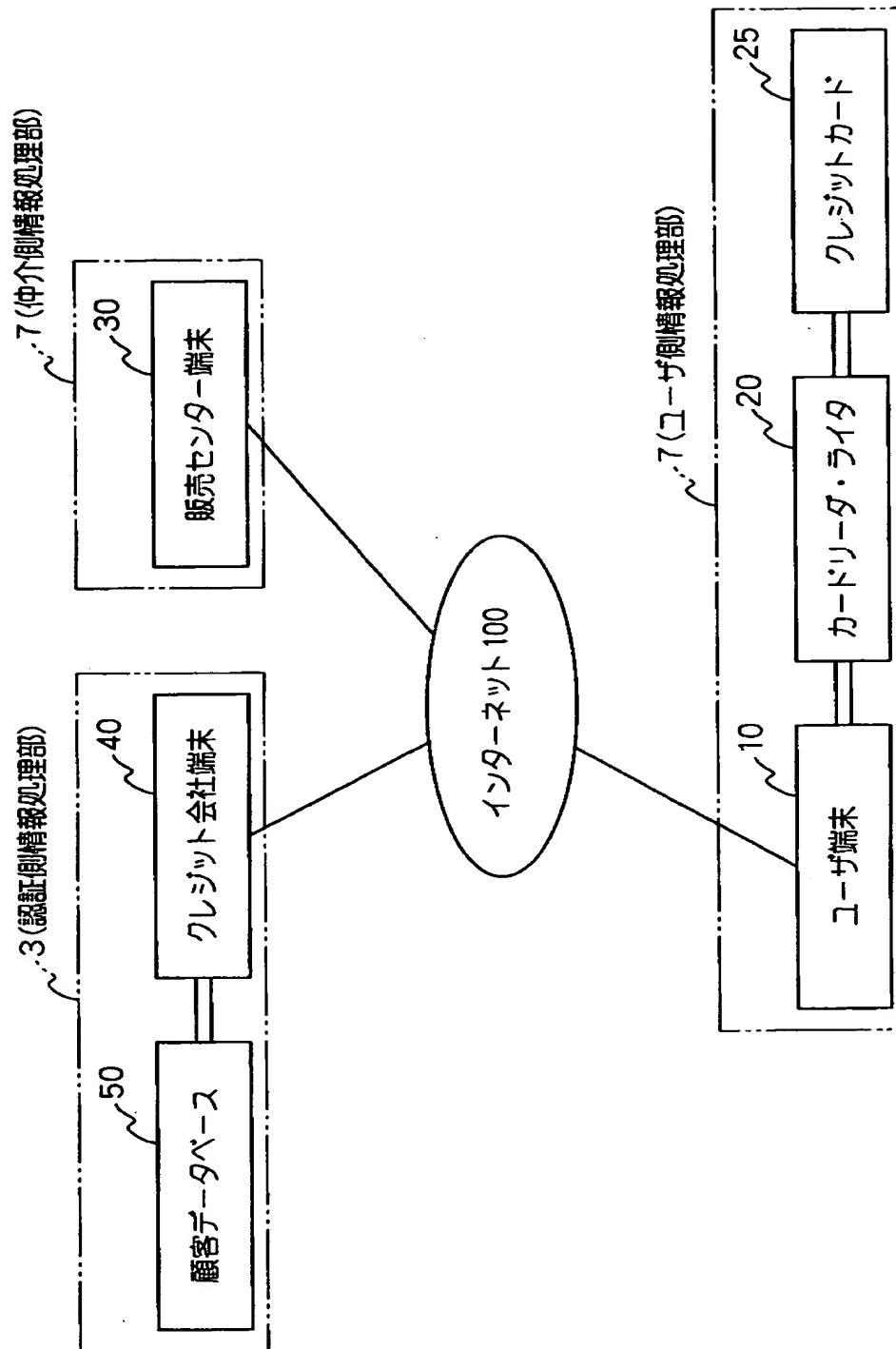
【図 7】



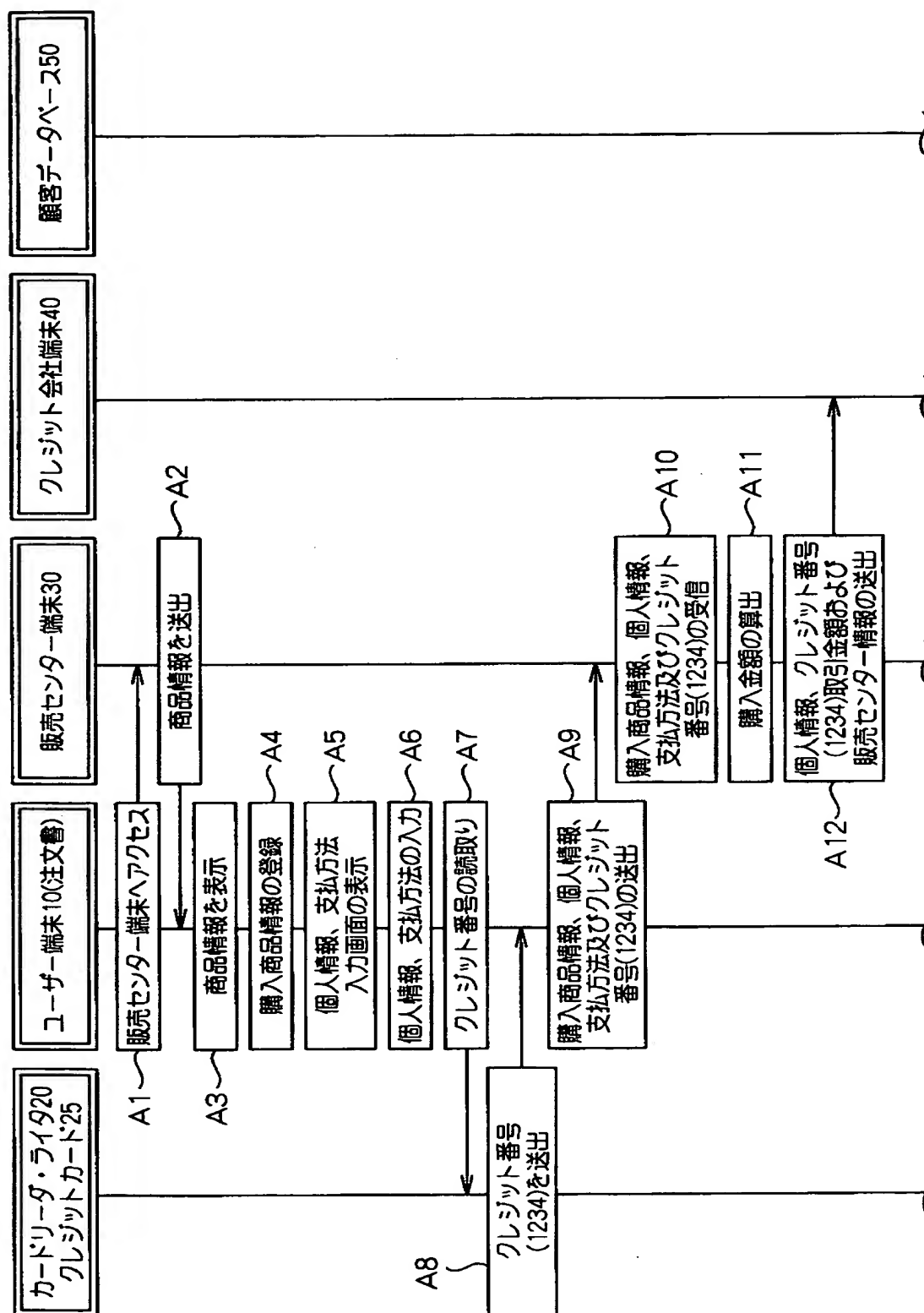
【図 8】



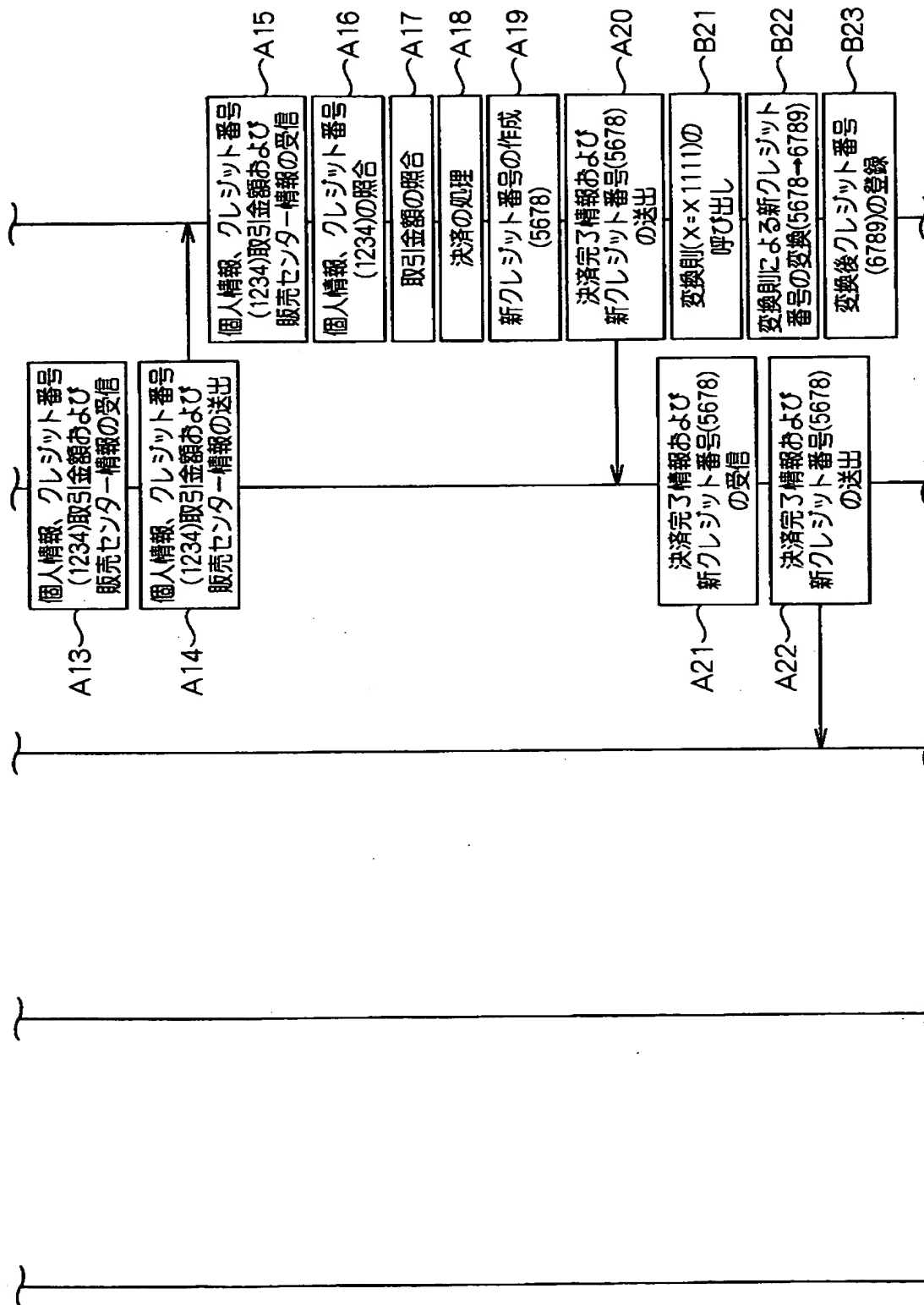
【図9】



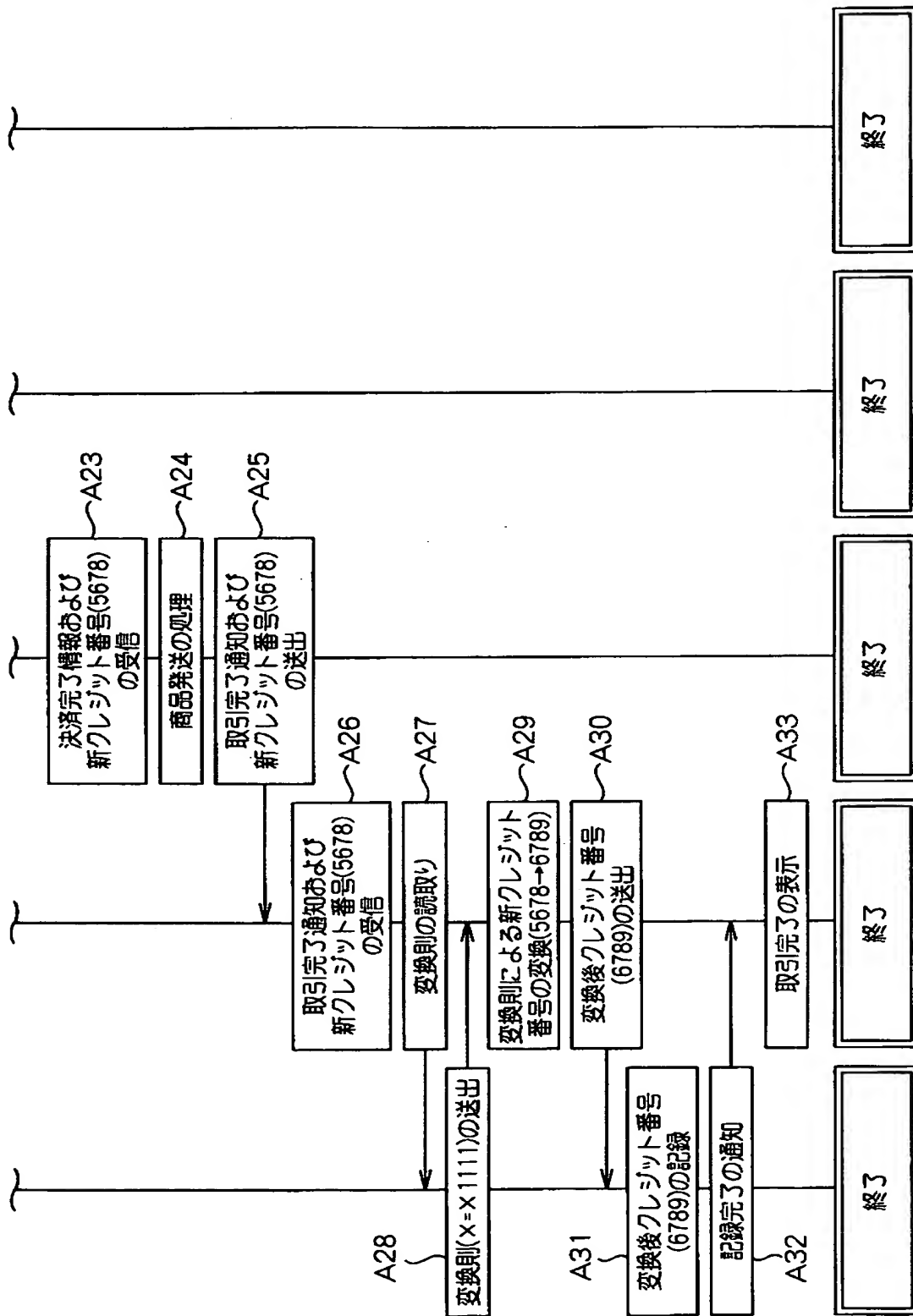
【図 10】



【図 11】



【図 12】



【図 13】

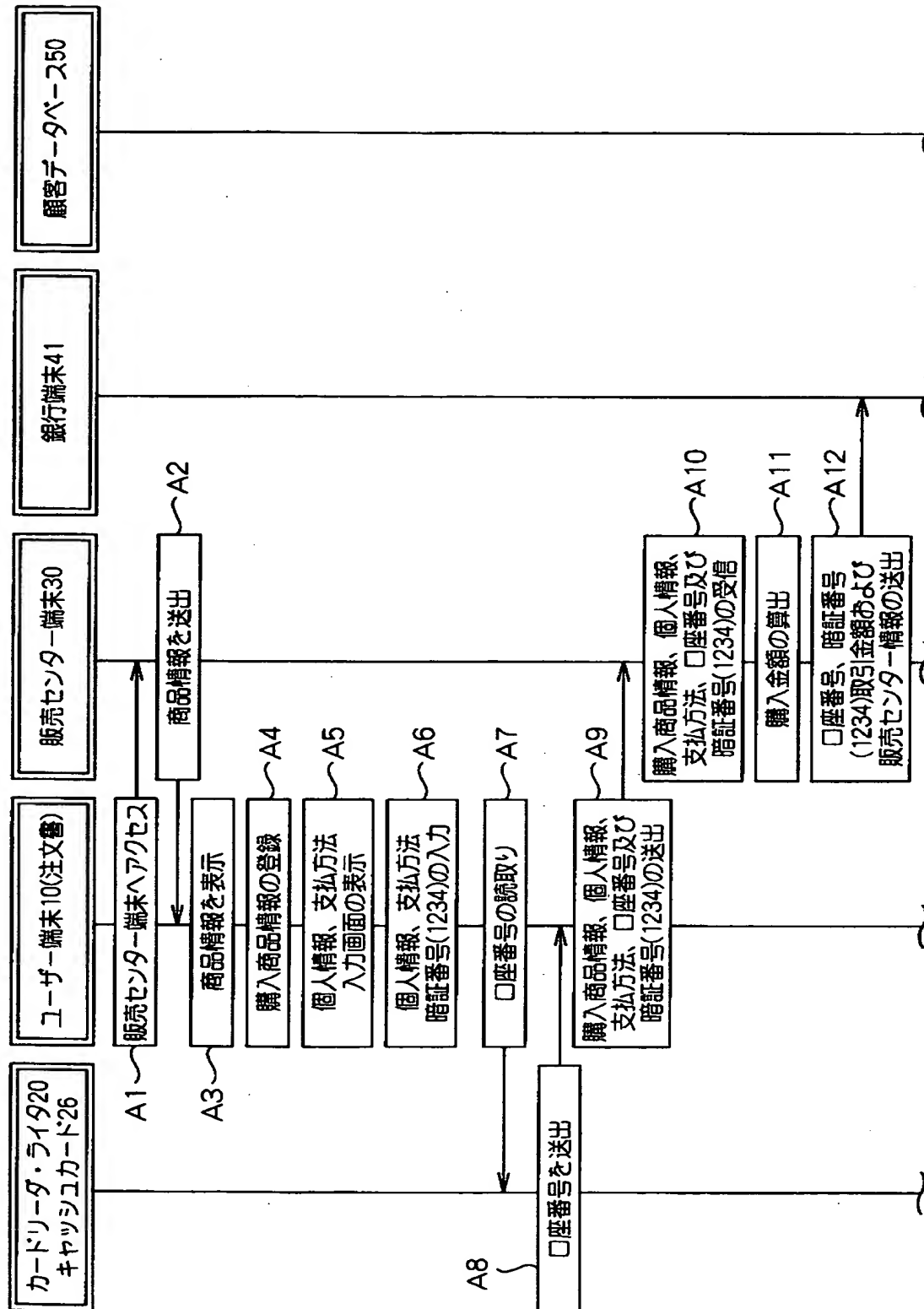
名称	商品番号	価格	購入
商品A	aaaa	¥3,000	<input type="checkbox"/>
商品B	bbbb	¥2,000	<input checked="" type="checkbox"/>
商品C	cccc	¥1,500	<input type="checkbox"/>
....			

〔1〕

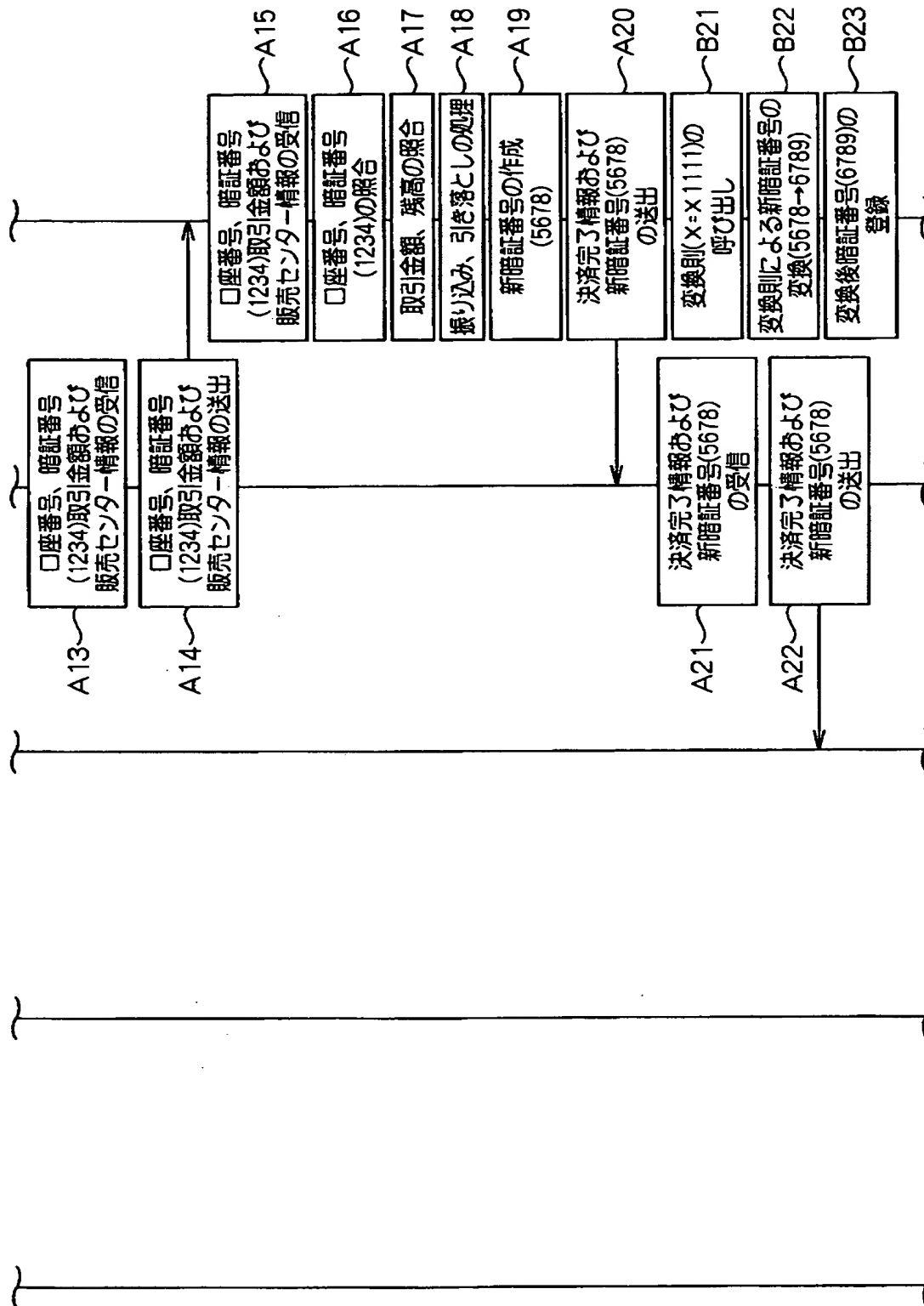
購入希望商品	:	商品B
住所	:	<input type="text" value="xxxxxxxxxxxx"/>
氏名	:	<input type="text" value="xxxxxx"/>
電話番号	:	<input type="text" value="xxxxxxxxxx"/>
支払方法	:	<input checked="" type="checkbox"/> クレジットカード <input type="checkbox"/> 銀行カード
		暗証番号: <input type="text"/>
<input type="button" value="送信"/>		

〔2〕

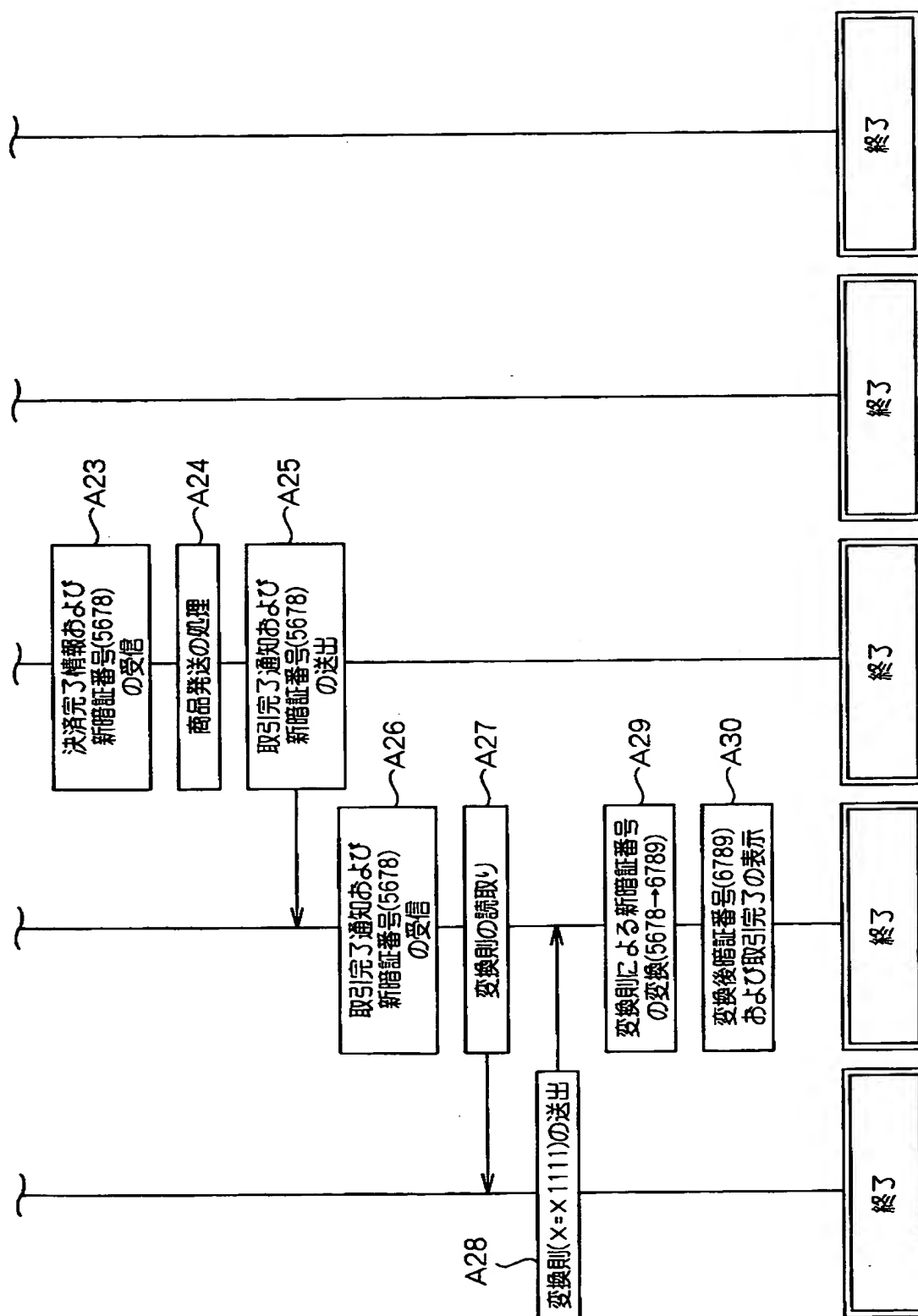
【図14】



【図 1 5】



【図16】



【書類名】 要約書

【要約】

【課題】 通信ネットワークを介して送受信されるクレジット番号等が第三者に盗まれた場合でも、悪用を防止する。

【解決手段】 ユーザ側情報処理部 2 は、第一の認証用番号を認証側情報処理部 3 へ送信する機能と、認証側情報処理部 3 からアクセス許可通知を受信すると、変換則 4 を用いて第一の認証用番号を第二の認証用番号に変換し、第二の認証用番号を新たな第一の認証用番号とする機能とを有する。認証側情報処理部 3 は、第一の認証用番号を受信すると、照合処理を実行する機能と、正規ユーザであればアクセス許可通知をユーザ側情報処理部 2 へ送信する機能と、変換則 4 と同じものを用いて第一の認証用番号を第二の認証用番号に変換し、第二の認証用番号を新たな第一の認証用番号としてデータベース 5 に記録する機能とを有する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000165033]

1. 変更年月日 1995年 5月17日
[変更理由] 住所変更
住 所 群馬県太田市西矢島町32番地
氏 名 群馬日本電気株式会社